

VOLUME 37, NUMBER 2, OCTOBER 2021

ALGEBRAS, GROUPS AND GEOMETRIES Volume 37, Number 2, October 2021

***ALGEBRAS,
GROUPS
AND
GEOMETRIES***

FOUNDED IN 1984. SOME OF THE PAST EDITORS
INCLUDE PROFESSORS: A. A. ANDERSEN,
V. V. DEODHAR, J. R. FAULKNER,
M. GOLDBERG, N. IWAHORI, M. KOECHER,
M. MARCUS, K. M. MCCRIMMON, R. V. MOODY,
R. H. OHEMKE, J. M. OSBORN, J. PATERA,
H. RUND, T. A. SPRINGER, G. S. TSAGAS.

EDITORIAL BOARD

M.R. ADHIKARI
A.K. ARINGAZIN
P. K. BANERJI
A. BAYOUMI
QING-MING CHENG
A. HARMANCY
L. P. HORWITZ
C. P. JOHNSON
S.L. KALLA
N. KAMIYA
J. LOHMUS*
R. MIRON
M.R. MOLAEI
P. NOWOSAD
KAR-PING SHUM
SERGEI SILVESTROV
H. M. SRIVASTAVA
G.T. TSAGAS*

* In memoriam

**FOUNDER and
Editor In Chief
R. M. SANTILLI**



HADRONIC PRESS, INC.

ALGEBRAS GROUPS AND GEOMETRIES

VOLUME 37, NUMBER 2, OCTOBER 2021

ISONUMBERS AND RGB IMAGE ENCRYPTION, 103

Mamadou I. Wade and Tepper L. Gill

EECS Howard University

Washington, DC, 20059 U.S.A.

ON THE LAPLACIAN SPECTRUM OF THE COMAXIMAL GRAPHS, 120

Mojgan Afkhami

Department of Mathematics, University of Neyshabur

P.O. Box 91136-899, Neyshabur, Iran

Zahra Barati

Department of Mathematics, Kosar University of Bojnord

Bojnord, Iran

Kazem Khashyarmanesh

Department of Pure Mathematics, Ferdowsi University of Mashhad

P.O. Box 1159-91775, Mashhad, Iran

THE NUMBER OF PRODUCTS OF N ELEMENTS IN A NONASSOCIATIVE ALGEBRA, 135

Simon Davis

Research Foundation of Southern California

8861 Villa La Jolla Drive #13595

La Jolla, CA 92039

FRUTE LOOPS, 159

Tèmítópé Gbóláhàn Jaiyéolá

Adesola Adefemi Adeniregun

Department of Mathematics, Obafemi Awolowo University

Ile Ife 220005, Nigeria

Oyeyemi Oluwaseyi Oyebola

Faculty of Education, Brandon University

Brandon Manitoba, Canada

Adedayo Oke Adelakun

Department of Physics, Federal University of Technology

Akure, Ondo State, Nigeria

**ANALYTICAL SOLUTION OF AN INDUCED FIBER GRATING
RELATIVE HUMIDITY SENSOR, 181**

Mahboubeh Dehghani Sanij and Hosein Rooholamininejad

Shahid Bahonar University, Physics Faculty

Kerman, Iran 7616914111

Ali Reza Bahrampour

Sharif University of Technology, Department of Physics

Tehran, Iran 1458889694

HALIDON RINGS AND THEIR APPLICATIONS, 193

A. Telveenus

Kingston University of London International Study Centre

Stable Block, Kingston Hill Campus

KT2 7LB, UK

**ADVANCING COMPUTATIONAL SPACE VALUE THEORY [CSV
T] FOR MULTIVALENT GAME MECHANICS, 239**

Jonah Lissner

Canadian Journal of Pure and Applied Sciences

Computational Intelligence Group, University of Manitoba

INDEX VOL. 37, 2021....259

ISONUMBERS AND RGB IMAGE ENCRYPTION

Mamadou I. Wade and Tepper L. Gill

EECS Howard University
Washington, DC, 20059 U.S.A.
mamadou.wade@howard.edu
tgill@howard.edu

Received June 20, 2020

Abstract

In this paper we first discuss isonumber theory, which was developed for applications in physics by R. M. Santilli. We then use isonumbers of the first kind and the Paillier cryptographic system to add an additional security degree of freedom to the image encryption scheme, which we call the Paillier-Senegalese encryption process.

Following standard procedures we first separate a given RGB image into its constituent channel images, use public encryption keys in conjunction with the Paillier-Senegalese encryption function, to encrypt each of the R, G, and B-channel pixel intensity values. The encrypted channel images can be then combined and compressed if necessary before transmission through a possibly unsecured communication channel. The transmitted encrypted image is subsequently recovered by a decryption process which uses the Paillier-Senegalese decryption function in conjunction with the private decryption keys.

We are conducting a number of the performance and security analyses on the recovered and encrypted images in order to study and verify their robustness relative to all desirable security metrics. The complete results of our study will be reported later, but preliminary evidence shows that, the use of isonumbers provide an additional security degree of freedom for the production of encrypted images.

1 Introduction

A number of image encryption schemes have been proposed in the past. Image encryption schemes based on chaos in dynamical systems have been proposed in [3], [15] and [19]. Pareek et al. [19], have developed an encryption scheme which uses a 80-bit encryption key to initialize two chaotic maps. G. Ye et al. [13], have proposed an encryption scheme based on electrocardiography and autoblocking to generate the initial keys, which removes the need for manual assignment. Singh et al. [16] have developed an Elliptic Curve Cryptosystem, which one applies to a group of pixels to obtain a corresponding cipher-image. In another direction, P. P. Dang and P. M. Chau [20], have discussed an encryption scheme which uses the Discrete Wavelet Transform (DWT) for image compression and the block cipher Data Encryption Standard (DES) to produce a secure image. Image encryption using Multi-orders of the Fractional Fourier Transforms has been proposed by R. Tao, X. Meng, and Y. Wang [21]. In this case, the summation of different orders of the inverse discrete Fractional Fourier transform (FRFT) is applied to the interpolated sub-images to create the encrypted image.

This paper explores the application of isonumber theory to red green blue (RGB) image encryption.

Purpose

In this paper we introduce the Paillier-Senegalese image encryption process using the Paillier cryptographic scheme and Santilli's Isonumber Theory of the first kind (see [10]). The isonumber theory replaces the unit "one" of normal arithmetic by a new unit called an "isounit", which provides an additional degree of freedom for the encryption process. We apply our approach to the encryption and decryption of images in the visible range of the electromagnetic spectrum.

The introduction of an isounit may be seen as a shared private encryption and decryption key. We also note that our scheme possesses both public-key and private-key characteristics, so it can be seen as a hybrid public-key and private-key system. The major contribution of this paper is the introduction

of an isounit as a private key and the development of this hybrid public-key and private-key cryptographic system, allowing the improvement of security by increasing the number of decryption keys required for an attacker to gain access to the transmitted images.

Content

The paper is organized as follows: In Section II, we introduce the Santilli's isonumbers theory of the first kind. In Section III, we combine the isonumbers with the Paillier cryptographic scheme to produce Paillier-Senegalese image cryptographic scheme. In Section IV we propose methods that will allow us to analyze the performance and security for our image encryption approach. Section V is devoted to our conclusion.

2 Santilli's Theory of Isonumbers

In this section, we provide a brief introduction to Santilli's Theory of Isonumbers. The origin of isonumbers can be traced at least back to 1978, when Santilli published the second volume of his fundamental work on the "Foundations of Theoretical Mechanics". He was studying the more realistic problem of local physical systems with dissipative forces as opposed to the mathematically beautiful but physically incorrect case of local systems without these forces. As first noted by Santilli, all of the nice mathematics and geometry developed in the twentieth century and used in physics to study elementary particles fails. The failure follows because the special theory of relativity does not apply for studies inside the proton (or inside a star), where particles move in dissipative media (and not in a vacuum).

While looking for a way to extend the ideal mathematics, making it more useful for physics, he discovered that all mathematical structures could be preserved by replacing the normal unit by a strictly positive definite unit, which need not be commutative and may depend on any number of physical variables, change with time and have as many derivatives as needed to reproduce experimental reality. This new unit he called an "isotope" (see [5], [7] and [8]). The simplest case is that of the real and complex numbers,

where the unit is the number one. Santilli began his study of this case with his seminal paper on “isonumbers” (see [5] and also [9]).

Our interest is limited to isonumbers. To make the transition easy, we consider the simplest example, which was used by Santilli to represent antiparticles as particles moving backwards in time, providing a rigorous foundation for an idea proposed by Feynman.

The real numbers is a field, which may be represented by a five-tuple $(\mathbb{R}, +, 0, \cdot, 1)$. Where zero is the unit for addition and one is the unit for multiplication. Santilli noticed that mathematicians implicitly use a sense of direction from left to right for $\mathbb{R}$, so that we should write it as a six-tuple $(\mathbb{R}, +, 0, \cdot, 1, \rightarrow)$. It now follows that, in practice, our real number system is not symmetric. Santilli’s solution was to propose a new representation of the real numbers $(\hat{\mathbb{R}}, +, 0, *, \hat{1}, \leftarrow)$, where the unit for addition is unchanged, but the new unit for multiplication is now $\hat{1} = -1$. Thus,

$$\hat{a} * \hat{b} = (-a)(-1)(-b) = -ab = \widehat{ab}. \quad (2.1)$$

Santilli called $(\hat{\mathbb{R}}, +, 0, *, \hat{1}, \leftarrow)$ the isotopic dual representation of the real numbers. This is an example of Santilli’s Isonumber Theory of the Second Kind, where the new unit, called isounit, is in the field (i.e. $(-1) = \hat{1} \in \mathbb{R}$). We are interested in Santilli’s Isonumber Theory of the First Kind, where the new isounit $\hat{I}$ is not in the field. Let the field $F(a, +, \cdot)$ be given (e.g., Z_p , with p prime) and let the isounit $\hat{I} = \hat{T}^{-1} \notin F$ be an invertible quantity. Let a new definition of multiplication be defined on F using $*$ $= \hat{T}$ (see [10]). This allows us to define a new field $\hat{F}(\hat{a}, +, *)$ (called isofield of the first kind), with elements called isonumbers and rules given by:

$$\begin{aligned} \hat{a} &= a\hat{I}, & \hat{a} * \hat{b} &= (a\hat{I})\hat{T}(b\hat{I}) = ab\hat{I} = \widehat{ab} \\ \hat{a} + \hat{b} &= (a\hat{I}) + (b\hat{I}) = (a + b)\hat{I} = \widehat{a + b}. \\ \hat{0} &= 0\hat{I} = 0 \end{aligned} \quad (2.2)$$

3 The Paillier-Senegalese Algorithm

The construction of the Paillier-Senegalese cryptographic algorithm is accomplished in a three step process. The first step is the generation of

the Paillier-Senegalese public and private isokeys required for encryption and decryption. The second step is the definition and use of the Paillier-Senegalese encryption function with the public isokeys to encrypt each of the pixel intensity value from a given set of R, G, and B-Channel images. The third step is the definition and use of the Paillier Senegalese decryption function with the private isokeys for the decryption phase, recovering the corresponding RGB images.

Let a RGB image be given with an 8-bit encoding for each channel. This means that the pixel intensity values are in the range $[0, (L - 1)]$, where is $L = 256$. These pixel intensity values for each channel image can be assumed to belong to the finite prime field $Z_p = \{0, 1, 2, \dots, (p - 1)\}$ of order $p = 257$ representing the closest prime number after $L = 256$,

The key generation, encryption and decryption phases are as follows:

3.1 Public and Private Keys Generation

We begin with the use of the Paillier cryptographic system for generating the public and private keys, which we use to generate our Paillier-Senegalese cryptographic system public and private isokeys.

3.1.1 Traditional Paillier public and private keys generation

We randomly choose two large prime numbers q and s , so that the greatest common divisor (gcd) of qs and $(q - 1)(s - 1)$ is 1, that is

$$gcd(qs, (q - 1)(s - 1)) = 1. \quad (3.1)$$

The condition is satisfied if q and s are primes with the same length. Our next step is to compute the public key N , and private key λ . This is done by defining $N = q \times s$ and, using the the least common multiple function lcm , to define λ by:

$$\lambda = lcm(q - 1, s - 1). \quad (3.2)$$

To compute the private decryption key μ , we generate a random integer $g \in Z_{N^2}^* = \{1, 2, \dots, (N^2 - 1)\}$ such that the order l , of g is a multiple of N .

The value of g can be also computed as $g = 1 + N$ when p and s have the same length. The private decryption key μ is then defined using the modulo operator mod , by:

$$\mu = \{[L(g^\lambda \text{ mod } (N^2))]^{-1}\} \text{ mod } (N), \quad (3.3)$$

where $L[U] = (U - 1) N^{-1}$. Hence, the privation key needed for decryption is (λ, μ) , while the public key needed for encryption is (N, g) .

3.1.2 Paillier-Senegalese Cryptographic System Public and Private keys Generation

The public and private isokeys for the Paillier-Senegalese cryptographic scheme are described in this section. First, we randomly generate two large prime numbers q and s , and randomly generate the isounit $\hat{I}$ outside Z_p . For proof of concept, we have randomly generated the 200 digit integer $\hat{I} = 91446193624825680120842585289199005703827325309092129498393744207361338371695567731788631147895697391520081713935620650244629828082900156163404995075142190905435955078225770963022485699534833574025767$.

We use it to compute the following parameters:

$$\hat{q} = q\hat{I} \quad (3.4)$$

$$\hat{s} = s\hat{I} \quad (3.5)$$

$$\hat{N} = \hat{q} * \hat{s} = q\hat{I} (\hat{I}^{-1}) s\hat{I} = (qs)\hat{I} = N\hat{I} \quad (3.6)$$

Given $\hat{N}$, the value of N can be computed as $N = \hat{N}/\hat{I}$. We can also compute $\hat{N}^{\hat{b}}$ needed for the encryption function using the isomultiplicative operation of the first kind $\hat{a}^{\hat{b}} = a^b\hat{I}$ as follows:

$$\hat{N}^{\hat{b}} = N^2\hat{I} \quad (3.7)$$

The values for $\hat{g}$ and $\hat{p}$ corresponding to g and p are given by

$$\hat{g} = \hat{I} + \hat{N} = \hat{I} + N\hat{I} = (1 + N)\hat{I} = g\hat{I} \quad (3.8)$$

$$\hat{p} = p\hat{I} \quad (3.9)$$

Note that given $\hat{g}$, the value of g can be computed as $g = \hat{g}/\hat{I}$. The function $L(U)$ becomes

$$\begin{aligned} L[\hat{U}] &= (\hat{U} - \hat{I}) * \hat{N}^{-1} = (U - 1) \hat{I}(\hat{I}^{-1})\hat{I}N^{-1} \\ &= [(U - 1) N^{-1}] \hat{I} = L[U]\hat{I}, \end{aligned} \quad (3.10)$$

The private decryption isokeys corresponding to μ and λ becomes

$$\hat{\mu} = \mu\hat{I} \quad (3.11)$$

$$\hat{\lambda} = lcm(\hat{g} - \hat{I}, \hat{s} - \hat{I}) \quad (3.12)$$

The private isokey $\hat{\lambda}$ is also given by

$$\hat{\lambda} = \lambda\hat{I} \quad (3.13)$$

When $\hat{\lambda}$ is known, λ can be obtained by $\lambda = \hat{\lambda}/\hat{I}$.

Hence, the pairs of public encryption isokey and private decryption isokey are $(\hat{g}, \hat{N})$ and $(\hat{\lambda}, \hat{\mu})$, respectively.

3.2 Paillier-Senegalese RGB Image Encryption Phase

This subsection introduces the traditional Paillier encryption scheme and the modification leading to the Paillier-Senegalese scheme for a given RGB image.

For the traditional Paillier encryption phase, let y_R , y_G , and y_B represent the pixel intensity values for the R, G, and B-channel images respectively. To encrypt each pixel intensity value in the Paillier scheme, one writes:

$$E(y_R) = g^{y_R} x_1^N \mod (N^2) \quad (3.14)$$

$$E(y_G) = g^{y_G} x_2^N \mod (N^2) \quad (3.15)$$

$$E(y_B) = g^{y_B} x_3^N \mod (N^2) \quad (3.16)$$

where $x_i, i = 1, 2, 3$ is a random number in $Z_N^* = \{1, 2, \dots, (N - 1)\}$. The encrypted values $E(y_R)$, $E(y_G)$, and $E(y_B)$ are outside of our range of $[0, (L - 1)]$. To map them back into this range, we apply the $\text{mod } [p]$ operation, where p is 257. These values belong to the encrypted channel images that can be transmitted or stored as described in [18], and can be computed as follows:

$$C_R = E(y_R) \text{ mod } (p) = \{[g^{y_R} x_1^N \text{ mod } (N^2)]\} \text{ mod } (p) \quad (3.17)$$

$$C_G = E(y_G) \text{ mod } (p) = \{[g^{y_G} x_2^N \text{ mod } (N^2)]\} \text{ mod } (p) \quad (3.18)$$

$$C_B = E(y_B) \text{ mod } (p) = \{[g^{y_B} x_3^N \text{ mod } (N^2)]\} \text{ mod } (p) \quad (3.19)$$

3.2.1 The Paillier-Senegalese Encryption Scheme

To obtain the Paillier-Senegalese encryption scheme, we replace the above equations by:

$$E(\hat{y}_R) = \hat{g}^{\hat{y}_R} * \hat{x}_1^{\hat{N}} \text{ mod } (\hat{N}^2) \quad (3.20)$$

$$E(\hat{y}_G) = \hat{g}^{\hat{y}_G} * \hat{x}_2^{\hat{N}} \text{ mod } (\hat{N}^2) \quad (3.21)$$

$$E(\hat{y}_B) = \hat{g}^{\hat{y}_B} * \hat{x}_3^{\hat{N}} \text{ mod } (\hat{N}^2) \quad (3.22)$$

where $\hat{x}_i = x_i \hat{I}, i = 1, 2, 3$ is a random isonumber in $\hat{Z}_N^*$, $\hat{g} = g \hat{I}$, etc. (see section 3.1).

Proposition 3.1. *Using the Paillier-Senegalese cryptographic system, we have*

$$E(\hat{y}) = E(y) \hat{I} \quad (3.23)$$

Proof. To encrypt y using Paillier encryption function, we can write

$$E(y) = g^y x^N \text{ mod } (N^2) \quad (3.24)$$

Let N^2 be a positive integer and $g^y x^N$ be a nonnegative integer. Using the division algorithm, we have

$$g^y x^N = qN^2 + E(y) \quad (3.25)$$

where $q = \lfloor \frac{g^y x^N}{N^2} \rfloor$, $0 \leq E(y) < N^2$,

where the symbol $\lfloor x \rfloor$ is the floor function which represents the largest integer less than or equal to x .

So using Eq. 3.25, Eq. 3.24 can be written as

$$E(y) = g^y x^N - \lfloor \frac{g^y x^N}{N^2} \rfloor \times N^2 \quad (3.26)$$

Multiplying both side of of Eq. 3.26 by $\hat{I}$ gives

$$E(y)\hat{I} = \left(g^y x^N - \lfloor \frac{g^y x^N}{N^2} \rfloor N^2 \right) \hat{I} \quad (3.27)$$

The right side of Eq. 3.23 can be written as

$$E(\hat{y}) = \hat{g}^{(\hat{y})} * \hat{x}^{(\hat{N})} \mod \hat{N}^2 \quad (3.28a)$$

$$= (g^{(y)} x^N) \hat{I} \mod (N^2 \hat{I}) \quad (3.28b)$$

$$= (g^{(y)} x^N) \hat{I} - \lfloor \frac{g^y x^N \hat{I}}{N^2 \hat{I}} \rfloor (N^2 \hat{I}) \quad (3.28c)$$

$$= \left[(g^{(y)} x^N) - \lfloor \frac{g^y x^N}{N^2} \rfloor N^2 \right] \hat{I} \quad (3.28d)$$

$$E(\hat{y}) = E(y)\hat{I} \quad (3.28e)$$

□

Using the result obtained from Eq. 3.28e, Eqs. 3.20 3.21, and 3.22 can be written as

$$E(\hat{y}_R) = E(y_R)\hat{I} \quad (3.29)$$

$$E(\hat{y}_G) = E(y_G)\hat{I} \quad (3.30)$$

$$E(\hat{y}_B) = E(y_B)\hat{I} \quad (3.31)$$

The computational cost of implementing Eqs. 3.29, 3.30, and 3.31 is less than the computational cost of Eqs. 3.20, 3.21, and 3.22.

Similar to the encryption of RGB images using the traditional Paillier encryption system as described on our previous papers [17], [18] the quantities

$E(\hat{y}_R)$, $E(\hat{y}_G)$, and $E(\hat{y}_B)$ are out of the range $[0, (L - 1)]$. They must be mapped to this range by applying $\text{mod } p$ to each as follows:

$$\hat{C}_R = E(\hat{y}_R) \text{ mod } (p) = [\hat{g}(\hat{y}_R) * \hat{x}_1^{(\hat{N})} \text{ mod } (\hat{N})^2] \text{ mod } (p) \quad (3.32)$$

$$\hat{C}_G = E(\hat{y}_G) \text{ mod } (p) = [\hat{g}(\hat{y}_G) * \hat{x}_2^{(\hat{N})} \text{ mod } (\hat{N})^2] \text{ mod } (p) \quad (3.33)$$

$$\hat{C}_B = E(\hat{y}_B) \text{ mod } (p) = [\hat{g}(\hat{y}_B) * \hat{x}_3^{(\hat{N})} \text{ mod } (\hat{N})^2] \text{ mod } (p) \quad (3.34)$$

The quantities $\hat{C}_R$, $\hat{C}_G$, and $\hat{C}_B$ represents the encrypted pixel intensity values that will be transmitted and/or stored.

Other parameter needed for the decryption are also computed as follows:

$$q_R = \left\lfloor \frac{E(\hat{y}_R)}{p} \right\rfloor \quad (3.35)$$

$$q_G = \left\lfloor \frac{E(\hat{y}_G)}{p} \right\rfloor \quad (3.36)$$

$$q_B = \left\lfloor \frac{E(\hat{y}_B)}{p} \right\rfloor \quad (3.37)$$

where the symbol $\lfloor \rfloor$ represents the floor function. The quantities given in Eqs. (3.35), (3.36), and (3.37) are not secret but can also be encrypted using other encryption methods to increase the security of the cipher images.

3.3 Paillier-Senegalese RGB Image Decryption Phase

This subsection presents the Traditional Paillier Cryptographic Decryption Approach and the Proposed Paillier-Senegalese Cryptographic Decryption Approach.

In our previous paper [17], the traditional Paillier Cryptographic scheme was used for the decryption of $E(y_R)$, $E(y_G)$, and $E(y_B)$ to obtain y_R , y_G , and y_B .

In particular the encrypted pixel intensity values C_R , C_G , and C_B , and the quotients given by $qt_R = \left\lfloor \frac{E(y_R)}{p} \right\rfloor$, $qt_G = \left\lfloor \frac{E(y_G)}{p} \right\rfloor$, $qt_B = \left\lfloor \frac{E(y_B)}{p} \right\rfloor$ are

assumed available to the decryption function at the receiver side. To reconstruct $E(y_R)$, $E(y_G)$, and $E(y_B)$ before applying the Paillier decryption function, we can write.

$$E(y_R) = qt_R \times p + C_R = \alpha \quad (3.38)$$

$$E(y_G) = qt_G \times p + C_G = \beta \quad (3.39)$$

$$E(y_B) = qt_B \times p + C_B = \gamma \quad (3.40)$$

To recover the original pixels' intensity values y_R , y_G , and y_B , the Paillier decryption function is applied to $E(y_R) = \alpha$, $E(y_G) = \beta$, and $E(y_B) = \gamma$ in Eqs. (3.38), (3.39), and (3.40) as follows:

$$y_R = \frac{L[\alpha^\lambda \bmod (N^2)]}{L[g^\lambda \bmod (N^2)]} \bmod (N) \quad (3.41)$$

$$y_G = \frac{L[\beta^\lambda \bmod (N^2)]}{L[g^\lambda \bmod (N^2)]} \bmod (N) \quad (3.42)$$

$$y_B = \frac{L[\gamma^\lambda \bmod (N^2)]}{L[g^\lambda \bmod (N^2)]} \bmod (N) \quad (3.43)$$

3.3.1 The Paillier-Senegalese Decryption Approach

Now, consider our proposed Paillier-Senegalese decryption method. Assume that the quantities q_R , q_G , and q_B are available to the decryption function in addition to $\hat{C}_R$, $\hat{C}_G$, and $\hat{C}_B$.

One must first reconstruct $E(\hat{y}_R)$, $E(\hat{y}_G)$, and $E(\hat{y}_B)$ from the receive cipher pixel values, $\hat{C}_R$, $\hat{C}_G$, and $\hat{C}_B$ before applying the decryption function as follows.

$$E(\hat{y}_R) = q_R \times p + \hat{C}_R = \hat{\alpha} \quad (3.44)$$

$$E(\hat{y}_G) = q_G \times p + \hat{C}_G = \hat{\beta} \quad (3.45)$$

$$E(\hat{y}_B) = q_B \times p + \hat{C}_B = \hat{\gamma} \quad (3.46)$$

The Paillier-Senegalese decryption function can be applied to $E(\hat{y}_R)$, $E(\hat{y}_G)$, and $E(\hat{y}_B)$, in Eqs. (3.44), (3.45), and (3.46) to recover the original

pixels' intensity values $\hat{y}_R$, $\hat{y}_G$, and $\hat{y}_B$, and then y_R , y_G , and y_B belonging to our original channel images. They are computed as follows:

$$\hat{y}_R = \frac{L[\hat{\alpha}^\lambda \bmod (\hat{N}^2)]}{L[\hat{g}^\lambda \bmod (\hat{N}^2)]} \bmod (\hat{N}) \quad (3.47)$$

$$\hat{y}_G = \frac{L[\hat{\beta}^\lambda \bmod (\hat{N}^2)]}{L[\hat{g}^\lambda \bmod (\hat{N}^2)]} \bmod (\hat{N}) \quad (3.48)$$

$$\hat{y}_B = \frac{L[\hat{\gamma}^\lambda \bmod (\hat{N}^2)]}{L[\hat{g}^\lambda \bmod (\hat{N}^2)]} \bmod (\hat{N}) \quad (3.49)$$

From equations 3.11 and 3.3, $L[\hat{g}^\lambda \bmod (\hat{N}^2)] = \hat{\mu} = \mu \hat{I}$, so that these equations can be written as:

$$\hat{y}_R = \left\{ L[\hat{\alpha}^\lambda \bmod (\hat{N}^2)] * \hat{\mu} \right\} \bmod (\hat{N}) \quad (3.50)$$

$$\hat{y}_G = \left\{ L[\hat{\beta}^\lambda \bmod (\hat{N}^2)] * \hat{\mu} \right\} \bmod (\hat{N}) \quad (3.51)$$

$$\hat{y}_B = \left\{ L[\hat{\gamma}^\lambda \bmod (\hat{N}^2)] * \hat{\mu} \right\} \bmod (\hat{N}) \quad (3.52)$$

To find $L[\hat{\alpha}^\lambda \bmod (\hat{N}^2)]$, let $\hat{U} = \hat{\alpha}^\lambda \bmod (\hat{N}^2)$. The value of $\hat{U}$ can also be computed as $\hat{U} = (\alpha^\lambda) \hat{I} \bmod (\hat{N}^2)$ and using Eq. 3.10 we have

$$L[\hat{\alpha}^\lambda \bmod (\hat{N}^2)] = L(\hat{U}) = \frac{(\hat{U} - \hat{I})}{N} \quad (3.53)$$

Another method of computing $L[\hat{\alpha}^\lambda \bmod (\hat{N}^2)]$ is given by

$$L[\hat{\alpha}^\lambda \bmod (\hat{N}^2)] = L(\hat{U}) = L(U) \hat{I} \quad (3.54)$$

where $L(U)$ is given in section 3.1.1 and $U = \alpha^\lambda \bmod N^2$, where $\alpha = \frac{\hat{\alpha}}{\hat{I}}$.

Similarly, let $\hat{U}_1 = \hat{g}^\lambda \bmod (\hat{N}^2)$. The expression of $\hat{U}_1$ can also be written as $\hat{U}_1 = (g^\lambda) \hat{I} \bmod (\hat{N}^2)$ and we can also write

$$L[\hat{g}^\lambda \bmod (\hat{N}^2)] = L(\hat{U}_1) = \frac{(\hat{U}_1 - \hat{I})}{N} \quad (3.55)$$

Furthermore, Eq. 3.55 is also given by

$$L[\hat{g}^{\hat{\lambda}} \bmod (\hat{N}^{\hat{2}})] = L(\hat{U}_1) = L(U_1)\hat{I} \quad (3.56)$$

where $L(U_1)$ is given in section 3.1.1 and $U_1 = g^{\lambda} \bmod (N^2)$. Similar analysis from Eq. 3.50 through Eq. 3.56 can be also apply to further compute the values of $\hat{y}_G$ and $\hat{y}_B$ in Eqs. 3.48 and 3.49. Now, the values of y_R , y_G , and y_B are given by

$$y_R = \frac{\hat{y}_R}{\hat{I}}, \quad y_G = \frac{\hat{y}_G}{\hat{I}}, \quad y_B = \frac{\hat{y}_B}{\hat{I}} \quad (3.57)$$

For software implementation purposes, it is more efficient to use matrices of pixels' intensity values instead of individual pixels.

4 CONCLUSION

In this paper, we have introduced the Paillier-Senegalese cryptographic scheme which combines the Santilli's Isonumber Theory of the first kind with the Paillier Cryptographic System to provide an additional degree of freedom to the encryption-decryption of RGB images. This leads to a Hybrid public private-key cryptographic system with a substantial increase in image security, which also may be used in a variety of applications for secure systems that may not be related to image encryption and decryption.

References

- [1] A. Soleymani, Md. J. Nordin, and Z. Md. Ali, *A Novel Public Key Image Encryption Based on Elliptic Curves over Prime Group Field*, Journal of Image and Graphics, Vol. 1, No. 1, March, 2013.
- [2] A. Kanso, M. Ghebleh, *A novel image encryption algorithm based on a 3D chaotic map*, Commun Nonlinear Sci Numer Simulat 17 (2012) 2943-2959,
www.elsevier.com/locate/cnsns
- [3] A. Daneshgar and B. Khadem, *A self-synchronized chaotic image encryption scheme*, Signal Processing: Image Communication 36 (2015) 106-114.
www.elsevier.com/local/image
- [4] A. K. A. Hassan, *Reliable Implementation of Paillier Cryptosystem*, Iraqi Journal of Applied Physics, IJAP, Vol. 10, No. 4, October-December 2014, pp. 27-29
- [5] R. M.Santilli-1, *Foundations of Theoretical Mechanics II*, Springer-Verlag New York, U.S.A, (1978), ISBN 0-387-08874-1.
- [6] R. M.Santilli-2, *Isonumbers and Genonumbers of Dimensions 1, 2, 4, 8, their Isoduals and Pseudoduals, and "Hidden Numbers," of Dimension 3, 5, 6, 7*, Algebras, Groups and Geometries, Vol. 10, 273 (1993).
- [7] R. M.Santilli-3, *Elements of Hadronic Mechanics I*, Ukraine Academy of Sciences, Kiev, (1995), Ukraine, ISBN 0-911767-68-1.
- [8] R. M.Santilli-4, *Isorepresentation of the Lie-isotopic $SU(2)$ Algebra with Application to Nuclear Physics and Local Realism*, Acta Applicandae Mathematicae Vol. 50, 177 (1998).
- [9] C. Corda, *Introduction to Santilli's IsoNumbers*, AIP Conf. Proceed. 1479, 1013 (2012),

- [10] C. X. Jiang, *Foundations of Santilli's Isonumber Theory*, Fundamental Open Problems in Science at the End of the Millennium, Proceeding of the Beijing Workshop, August 1997, Hadronic Press, Palm Harbor, FL 34682-1577, U.S.A, ISBN 1-57485-029-6, PP. 105-139, Edited by Tepper Gill (Co-author of this paper), K. Liu, and E. Trell.
- [11] G. Zhang, and Q. Liu, *A novel image encryption method based on total shuffling scheme*, Optics Communications 284 (2011) 2775-2780, www.elsevier.com/locate/optcom
- [12] G. Chen, Y. Mao, and C. K. Chui, *A symmetric image encryption scheme based on 3D chaotic cat maps*, Chaos, Solitons and Fractals 21 (2004) 749-761, www.elsevier.com/locate/chaos
- [13] G. Ye and X. Huang, *An Image Encryption Algorithm Based on Autoblocking and Electrocardiography*, Published by the IEEE Computer Society. April-June 2016.
- [14] H. Liu, X. Wang, and A. kadir, *Image encryption using DNA complementary rule and chaotic maps*, Applied Soft Computing 12 (2012) 1457-1466, www.elsevier.com
- [15] H. S. Kwok, Wallace K. S. Tang, *A fast image encryption system based on chaotic maps with finite precision representation*, Chaos, Solitons and Fractals 32 (2007) 1518-1529, www.elsevier.com/locate/chaos
- [16] L. D. Singh and K. M. Singh, *Image Encryption using Elliptic Curve Cryptography*, Procedia Science 54 (2015) 475-481, www.sciencedirect.com
- [17] M. I. Wade, H. C. Ogworonjo, M. Gul, M. Ndoye, M. Chouikha, W. Paterson *Red Green Blue Image Encryption Based on Paillier Cryptographic Cryptographic Approach*, World Academy of Science, Engineering and Technology, International Journal of Electronics and Commu-

nication Engineering Vol:11, No:12, 2017,
<https://waset.org/abstracts/79232>

- [18] M. I. Wade, *Distributed Image Encryption Based On a Homomorphic Cryptographic Approach*, 10th IEEE Annual Ubiquitous Computing, Electronics and Mobile Communication Conference, Columbia University, New York City, USA 10- 12 October 2019 (IEEE UEMCON 2019).
- [19] N. K. Pareek, V. Patidar, and K. K. Sud, *Image Encryption Using Chaotic Logistic Map*, *Image and Vision Computing* 24 (2006) 926-934,
www.elsevier.com/locate/optlaseng
- [20] P. P. Dang and P. M. Chau, *Image Encryption for Secure Internet Multimedia Applications*, *IEEE Trans. On Consumer Electronics*, Vol. 46. No. 3, August 2000.
- [21] R. Tao, X. Meng, and Y. Wang, *Image Encryption With Multiorders of Fractional Fourier Transforms*, *IEEE Trans. Inf. Forensics and Security*, Vol. 5, No 4, Dec 2010.
- [22] R. Rivest, Lecture Notes 15, Computer and Network Security: *Voting, Homomorphic Encryption*, October, 2002.
- [23] R. C. Gonzalez and R. E. Woods, *Digital Image Processing*, 3rd ed. Person Education Inc., 2008.
- [24] R. Rhouma, S. Meherzi, and S. Belghith, *OCML-based colour image encryption*, *Chaos, Solitons and Fractals* 40 (2009) 309-318,
www.elsevier.com/locate/chaos
- [25] S. Mazloom and A. M. E-Moghadam, *Color image encryption based on Coupled Nonlinear Chaotic Map*, *Chaos, Solitons and Fractals* 42 (2009) 1745-1754,
www.elsevier.com/locate/chaos
- [26] *University of Southern California, Signal and Image Processing Institute*,
<http://sipi.usc.edu/database/>

- [27] Y. Zhou, L. Bao, C. L. P. Chen *A new 1D chaotic system for image encryption*, Signal Processing 97 (2014) 172–182,
www.elsevier.com/locate/sigpro
- [28] Yi. Xun, P. Russell, and B. Elisa, *Homomorphic Encryption and Applications*, 2014 XII, 126 p. 23 illus.,
<http://www.springer.com/978-3-319-12228-1>

ON THE LAPLACIAN SPECTRUM OF THE COMAXIMAL GRAPHS

Mojgan Afkhami

Department of Mathematics, University of Neyshabur
P.O. Box 91136-899, Neyshabur, Iran
mojgan.afkhami@yahoo.com

Zahra Barati

Department of Mathematics, Kosar University of Bojnord
Bojnord, Iran
za.barati87@gmail.com

Kazem Khashyarmansh

Department of Pure Mathematics, Ferdowsi University of Mashhad
P.O. Box 1159-91775, Mashhad, Iran
khashyar@ipm.ir

Received June 4, 2021

Abstract

Assume that R is a commutative ring. The comaximal graph of R , denoted by $\Gamma(R)$, is a simple graph whose vertex set consists of all elements of R , and two distinct vertices a and b are adjacent if and only if $Ra + Rb = R$. In this paper, we investigate the Laplacian spectrum of the comaximal graph of the ring $\mathbb{Z}_n$. We show that $\Gamma(\mathbb{Z}_n)$ is decomposable if and only if $n = p^\alpha q^\beta$, for every prime numbers p and q and integers $\alpha, \beta \geq 0$, and then we prove that $\Gamma(\mathbb{Z}_{p^\alpha q^\beta})$ is Laplacian integral. We also show that the Laplacian spectral radius of $\Gamma(\mathbb{Z}_n)$ is equal to n , and the vertex connectivity and algebraic connectivity of $\Gamma(\mathbb{Z}_n)$ are equal to $\phi(n)$, where ϕ is the Euler's totient function.

AMS Classification 05C25, 05C50, 05C75

Keywords. Comaximal graph, Laplacian spectrum, Laplacian spectral radius, Algebraic connectivity, Vertex connectivity

1 Introduction

Let G be a simple graph with n vertices, whose vertex set is $V(G) = \{v_1, v_2, \dots, v_n\}$. For a vertex v of G , $N_G(v)$ denotes the set of vertices of G that are adjacent to v in G , and we denote $|N_G(v)|$ by $\deg(v)$. For two distinct vertices v_i and v_j of G , we write $v_i \sim v_j$ if v_i and v_j are adjacent in G . The *adjacency matrix* of G is the $n \times n$ matrix $A(G) = (a_{ij})$, where $a_{ij} = 1$ if $v_i \sim v_j$, and otherwise $a_{ij} = 0$. Also, $D(G)$ is the diagonal matrix with the (v, v) th entry having value $\deg v$. The *Laplacian matrix* $L(G)$ of G is defined by $L(G) = D(G) - A(G)$, and the eigenvalues of $L(G)$ are called the *Laplacian eigenvalues* of G . Clearly, $L(G)$ is a real, symmetric, and positive semidefinite matrix, and so all its eigenvalues are real and nonnegative. Also, the sum of the entries in each row of $L(G)$ is zero, and hence the smallest eigenvalue of $L(G)$ is zero with corresponding eigenvector $[1, 1, \dots, 1]^T$. Like the Laplacian matrix of a graph, the signless Laplacian matrix is positive semidefinite.

The *spectrum* of a square matrix B , denoted by $\sigma(B)$, is the multiset of all the eigenvalues of B . Let $\mu_1, \mu_2, \dots, \mu_r$ be distinct eigenvalues of B with multiplicities $m_1, m_2, \dots, m_r$, respectively. Then we denote the spectrum of B by

$$\sigma(B) = \begin{pmatrix} \mu_1 & \mu_2 & \dots & \mu_r \\ m_1 & m_2 & \dots & m_r \end{pmatrix}.$$

For a graph G , the spectrum of $L(G)$, is called the *Laplacian spectrum* and it is denoted by $\sigma_L(G)$. The Laplacian spectrum of graphs have been widely studied in [3, 12]. Assume that G has n vertices and m edges, and let $\mu_1, \mu_2, \dots, \mu_n$ be the Laplacian eigenvalues of G . Then the *Laplacian energy* of G is defined as

$$\text{LE}(G) = \sum_{i=1}^n \left| \mu_i - \frac{2m}{n} \right|.$$

In a graph G , $V(G)$ and $E(G)$ denote the vertex set and edge set of G , respectively. Also $\overline{G}$ denotes the complement of G . We say that G is an *empty graph* if $E(G) = \emptyset$ and it is a *null graph* if $V(G) = \emptyset$. A vertex v is an isolated vertex if $\deg v = 0$. Also, K_n denotes the complete graph on n vertices and P_n denotes the path with n vertices.

The Laplacian spectrum of the complete graph K_n and its complement $\overline{K_n}$ are known. Indeed,

$$\sigma_L(K_n) = \begin{pmatrix} 0 & n \\ 1 & n-1 \end{pmatrix} \text{ and } \sigma_L(\overline{K_n}) = \begin{pmatrix} 0 \\ n \end{pmatrix}.$$

Let G_1 and G_2 be two graphs with disjoint vertex sets. Then the *union of the graphs* G_1 and G_2 , which is denoted by $G_1 \cup G_2$, is a graph with the vertex set $V(G_1) \cup V(G_2)$ and the edge set $E(G_1) \cup E(G_2)$, that is, the disjoint union of two graphs G_1 and G_2 . Also, let $\alpha_1, \alpha_2, \dots, \alpha_r$ and $\beta_1, \beta_2, \dots, \beta_s$ be the Laplacian eigenvalues of G_1 and G_2 , respectively. Then, by [12], the Laplacian eigenvalues of $G_1 \cup G_2$ is $\alpha_1, \alpha_2, \dots, \alpha_r, \beta_1, \beta_2, \dots, \beta_s$.

Let R be a commutative ring with nonzero identity. We denote the set of all unit elements and zero divisors of R by $U(R)$ and $Z(R)$, respectively. Also by $Z^*(R)$ we denote the set $Z(R) - \{0\}$. Sharma and Bhatwadekar [14] defined the comaximal graph of a commutative ring R , which is denoted by $\Gamma(R)$. The *comaximal graph* of R is a simple graph whose vertices consists of all elements of R , and two distinct vertices a and b are adjacent if and only if $aR + bR = R$, where cR is the ideal generated by c , for $c \in R$. Let $\Gamma_2(R)$ be an induced subgraph of $\Gamma(R)$ with nonunit elements of R as vertices. Some properties of the graph $\Gamma_2(R)$ were studied in [9], [15] and [16]. In this paper, we denote the graph $\Gamma_2(R) - \{0\}$ by $\Gamma_2^*(R)$.

Let $n > 1$ be an integer and let $\mathbb{Z}_n$ denote the ring of integers modulo n . Recently, in [2], the authors studied the Laplacian eigenvalues of the zero divisor graph of $\mathbb{Z}_n$.

In Section 2 of this paper, we study the structure of the comaximal graph of $\mathbb{Z}_n$. We show that $\Gamma_2^*(\mathbb{Z}_n)$ is a generalized join of some certain empty graphs. In the third section, we investigate and discuss the Laplacian spectrum and Laplacian energy of $\Gamma(\mathbb{Z}_n)$. In Section 4, we show that $\Gamma(\mathbb{Z}_n)$ is decomposable if and only if $n = p^\alpha q^\beta$, for every prime numbers p and q and integers $\alpha, \beta \geq 0$, and then we prove that $\Gamma(\mathbb{Z}_{p^\alpha q^\beta})$ is Laplacian integral. We also show that the Laplacian spectral radius of $\Gamma(\mathbb{Z}_n)$ is equal to n , and the vertex connectivity and algebraic connectivity of $\Gamma(\mathbb{Z}_n)$ are equal to $\phi(n)$, where ϕ is the Euler's totient function.

2 Structure of $\Gamma_2^*(\mathbb{Z}_n)$ and $\Gamma(\mathbb{Z}_n)$

In this paper, for two integers r and s , the notation (r, s) stands for the greatest common divisor of r and s . Also we denote the elements of the ring $\mathbb{Z}_n$, where $n > 1$, by $0, 1, 2, \dots, n-1$. For every nonzero element a in $\mathbb{Z}_n$, if $(a, n) = 1$, then a is a unit element; otherwise, $(a, n) \neq 1$, and so a is a zerodivisor. Therefore, $|U(\mathbb{Z}_n)| = \phi(n)$ and $|Z(\mathbb{Z}_n)| = n - \phi(n)$, where ϕ is the Euler's totient function.

An integer d is said to be a *proper divisor* of n if $1 < d < n$ and $d \mid n$.

Now let $d_1, d_2, \dots, d_k$ be the distinct proper divisors of n . For $1 \leq i \leq k$, set

$$A_{d_i} := \{x \in \mathbb{Z}_n \mid (x, n) = d_i\}.$$

Clearly, the sets $A_{d_1}, A_{d_2}, \dots, A_{d_k}$ are pairwise disjoint and we have

$$Z^*(\mathbb{Z}_n) = A_{d_1} \cup A_{d_2} \cup \dots \cup A_{d_k}$$

and

$$V(\Gamma(\mathbb{Z}_n)) = \{0\} \cup A_{d_1} \cup A_{d_2} \cup \dots \cup A_{d_k} \cup U(\mathbb{Z}_n).$$

The following lemma is stated from [17].

Lemma 2.1. [17, Proposition 2.1] *Let $1 \leq i \leq k$. Then $|A_{d_i}| = \phi(\frac{n}{d_i})$.*

In the rest of the paper, the induced subgraph of $\Gamma(\mathbb{Z}_n)$ on the set A_{d_i} is denoted by $\Gamma(A_{d_i})$, where $1 \leq i \leq k$.

In the following lemma, we investigate some adjacencies in $\Gamma(\mathbb{Z}_n)$.

Lemma 2.2. *The following statements hold:*

- (i) *Two distinct vertices x and y are adjacent in $\Gamma(\mathbb{Z}_n)$ if and only if $(x, y) \in U(\mathbb{Z}_n)$.*
- (ii) *For $1 \leq i \leq k$, $\Gamma(A_{d_i})$ is isomorphic to $\overline{K}_{\phi(\frac{n}{d_i})}$.*
- (iii) *For $1 \leq i \neq j \leq k$, a vertex of A_{d_i} is adjacent to a vertex of A_{d_j} if and only if $(d_i, d_j) = 1$.*

Proof. (i) First suppose that x and y are adjacent vertices in $\Gamma(\mathbb{Z}_n)$. Assume on the contrary that $d = (x, y) \notin U(\mathbb{Z}_n)$. So we have $x\mathbb{Z}_n \subseteq d\mathbb{Z}_n$ and $y\mathbb{Z}_n \subseteq d\mathbb{Z}_n$. Thus $x\mathbb{Z}_n + y\mathbb{Z}_n \subseteq d\mathbb{Z}_n \neq \mathbb{Z}_n$, and this means that x and y are not adjacent, which is a contradiction. Now, let $u = (x, y) \in U(\mathbb{Z}_n)$. So there exist $r, s \in \mathbb{Z}$ such that $u = rx + sy \in x\mathbb{Z}_n + y\mathbb{Z}_n$. Therefore we have $x\mathbb{Z}_n + y\mathbb{Z}_n = \mathbb{Z}_n$, which implies that x and y are adjacent.

(ii) For each two distinct elements $x, y \in A_{d_i}$, we have $(x, n) = d_i = (y, n)$. So $d_i \mid (x, y)$, which implies that $(x, y) \notin U(\mathbb{Z}_n)$. Hence by (i), we have that x and y are not adjacent. Therefore by Lemma 2.1, we have $\Gamma(A_{d_i}) \cong \overline{K}_{\phi(\frac{n}{d_i})}$.

(iii) Let $i, j \in \{1, 2, \dots, k\}$ with $i \neq j$. First assume that $x \in A_{d_i}$ and $y \in A_{d_j}$ are adjacent vertices. If $(d_i, d_j) = d \neq 1$, then $(n, d) = d$. Since $(x, n) = d_i$ and $(y, n) = d_j$, we have that $d \mid x, y$. Hence $Rx + Ry \subseteq Rd \neq R$, which is impossible. Now suppose that $(d_i, d_j) = 1$. Let $x \in A_{d_i}$ and $y \in A_{d_j}$

be arbitrary vertices. If $d = (x, y) \notin U(\mathbb{Z}_n)$, then $t = (d, n) \neq 1$. Since $t \mid x, y, n$, we have $t \mid (d_i, d_j)$ and this is impossible. Hence $(x, y) \in U(\mathbb{Z}_n)$ which means that x and y are adjacent. $\square$

In the following, we introduce a simple graph G_n , which plays an important role in the rest of the paper. The graph G_n is the simple graph with vertex set $\{d_1, d_2, \dots, d_k\}$, where d_i 's, $1 \leq i \leq k$, are the proper divisors of n , and two distinct vertices d_i and d_j are adjacent if and only if $(d_i, d_j) = 1$.

Let $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_t^{\alpha_t}$ be the factorization of n to its prime powers, where $t, \alpha_1, \dots, \alpha_t$ are positive integers and $p_1, \dots, p_t$ are distinct prime numbers. Every divisor of n is of the form $p_1^{\beta_1} p_2^{\beta_2} \dots p_t^{\beta_t}$, for some integers $\beta_1, \dots, \beta_t$, where $0 \leq \beta_i \leq \alpha_i$ for each $i \in \{1, 2, \dots, t\}$. Hence the number of proper divisors of n is equal to $\prod_{i=1}^t (\alpha_i + 1) - 2$. Therefore we have $k = |V(G_n)| = \prod_{i=1}^t (\alpha_i + 1) - 2$.

Recall that for two graphs H_1 and H_2 with disjoint vertex sets, the *join* $H_1 \vee H_2$ of the graphs H_1 and H_2 is the graph obtained from the union of H_1 and H_2 by adding new edges from each vertex of H_1 to every vertex of H_2 . The concept of join graph is generalized (in [13], it is called as a generalized composition graph). Assume that G is a graph on k vertices with $V(G) = \{v_1, v_2, \dots, v_k\}$, and let $H_1, H_2, \dots, H_k$ be k pairwise disjoint graphs. The G -generalized join graph $G[H_1, H_2, \dots, H_k]$ of $H_1, H_2, \dots, H_k$ is the graph formed by replacing each vertex v_i of G by the graph H_i and then joining each vertex of H_i to each vertex of H_j whenever $v_i \sim v_j$ in the graph G . Now, if the graph G consists of two adjacent vertices, then the G -generalized join graph $G[H_1, H_2]$ coincides with the join $H_1 \vee H_2$ of the graphs H_1 and H_2 .

In the following lemma, we state that $\Gamma_2^*(\mathbb{Z}_n)$ is a generalized join of some certain empty graphs.

Lemma 2.3. *In the comaximal graph of $\mathbb{Z}_n$, we have*

$$\Gamma_2^*(\mathbb{Z}_n) = G_n[\overline{K}_{\phi(\frac{n}{d_1})}, \overline{K}_{\phi(\frac{n}{d_2})}, \dots, \overline{K}_{\phi(\frac{n}{d_k})}]$$

and

$$\Gamma(\mathbb{Z}_n) = (K_1 \cup \Gamma_2^*(\mathbb{Z}_n)) \vee K_{\phi(n)}.$$

Proof. Consider the graph G_n and replace each vertex d_i of G_n by $\Gamma[A_{d_i}]$. In view of Lemma 2.1, we have

$$\Gamma_2^*(\mathbb{Z}_n) = G_n[\overline{K}_{\phi(\frac{n}{d_1})}, \overline{K}_{\phi(\frac{n}{d_2})}, \dots, \overline{K}_{\phi(\frac{n}{d_k})}].$$

Now, since the zero element is adjacent to only unit elements and each unit element is adjacent to all vertices in $\Gamma(\mathbb{Z}_n)$, we have

$$\Gamma(\mathbb{Z}_n) = (K_1 \cup \Gamma_2^*(\mathbb{Z}_n)) \vee K_{\phi(n)}.$$

□

Example 2.4. Consider the ring $\mathbb{Z}_{12}$. We have $d_1 = 2, d_2 = 3, d_3 = 4$, and $d_4 = 6$. Then G_{12} is the graph $2 \sim 3 \sim 4 \cup \{6\}$, which is isomorphic to $P_3 \cup K_1$. Now by Lemma 2.3, we have

$$\Gamma_2(\mathbb{Z}_{12}) = K_1 \cup G_{12}[\overline{K}_2, \overline{K}_2, \overline{K}_2, K_1].$$

3 Laplacian spectrum and Laplacian energy of $\Gamma(\mathbb{Z}_n)$

In this section, we describe the Laplacian spectrum of the comaximal graph of $\mathbb{Z}_n$. We also discuss the Laplacian spectrum and the Laplacian energy of $\Gamma(\mathbb{Z}_n)$, for some values of n .

In the next theorem, the Laplacian spectrum of the join of two graphs is determined.

Theorem 3.1. [11, Theorem 2.1] Let H_1 and H_2 be graphs on disjoint vertex sets with r and s vertices, respectively. If $\mu_1, \dots, \mu_r$ and $\nu_1, \dots, \nu_s$ are the Laplacian eigenvalues of H_1 and H_2 , respectively, then the Laplacian eigenvalues of $H_1 \vee H_2$ are $n = r + s$, $\mu_1 + s, \dots, \mu_{r-1} + s$, $\nu_1 + r, \dots, \nu_{s-1} + r$ and 0.

In the following theorem, which was proved by Cardoso et al. in [1, Theorem 8], the Laplacian spectrum of a generalized join graph $G[H_1, \dots, H_k]$ is determined in terms of the Laplacian spectrum of the graphs H_i 's and the spectrum of another $k \times k$ matrix $\mathcal{L}(G)$.

Theorem 3.2. [1] Let G be a graph with vertex set $\{v_1, v_2, \dots, v_k\}$ and let $H_1, H_2, \dots, H_k$ be k pairwise disjoint graphs with $m_1, m_2, \dots, m_k$ vertices, respectively. Then the Laplacian spectrum of $G[H_1, H_2, \dots, H_k]$ is given by

$$\sigma_L(G[H_1, H_2, \dots, H_k]) = \left(\bigcup_{j=1}^k (M_j + (\sigma_L(H_j) \setminus \{0\})) \right) \cup \sigma(\mathcal{L}(G)),$$

where

$$M_j = \begin{cases} \sum_{v_i \sim v_j} m_i & \text{if } N_G(v_j) \neq \emptyset, \\ 0 & \text{otherwise,} \end{cases}$$

$$\mathcal{L}(G) = \begin{bmatrix} M_1 & -s_{1,2} & \dots & -s_{1,k} \\ -s_{1,2} & M_2 & \dots & -s_{2,k} \\ \dots & \dots & \ddots & \dots \\ -s_{1,k} & -s_{2,k} & \dots & M_k \end{bmatrix},$$

and

$$s_{i,j} = \begin{cases} \sqrt{m_i m_j} & \text{if } v_i \sim v_j \text{ in } G, \\ 0 & \text{otherwise.} \end{cases}$$

Note that $\sigma_L(H_j) \setminus \{0\}$ means that one copy of the eigenvalue 0 is removed from the multiset $\sigma_L(H_j)$, and $M_j + (\sigma_L(H_j) \setminus \{0\})$ means that M_j is added to each element of $\sigma_L(H_j) \setminus \{0\}$.

Let G be a vertex weighted graph by assigning the weight $m_i = |V(H_i)|$ to the vertex v_i of G , for $1 \leq i \leq k$. Let $W(G) = (w_{i,j})$ be the $k \times k$ matrix, where

$$w_{i,j} = \begin{cases} -m_j & \text{if } i \neq j \text{ and } v_i \sim v_j, \\ \sum_{v_i \sim v_r} m_r & \text{if } i = j, \\ 0 & \text{otherwise.} \end{cases}$$

The matrix $W(G)$ is called a vertex weighted Laplacian matrix of G . In [4, p. 317], it is shown that the matrices $W(G)$ and $\mathcal{L}(G)$ are similar, and so we have $\sigma(\mathcal{L}(G)) = \sigma(W(G))$. Hence in Theorem 3.2, we can use $\sigma(W(G))$ instead of $\sigma(\mathcal{L}(G))$ for determining the Laplacian spectrum of $G[H_1, H_2, \dots, H_k]$.

Suppose that $d_1, d_2, \dots, d_k$ are the proper divisors of n . We assign the weight $|A_{d_j}| = \phi(\frac{n}{d_j})$, for $1 \leq j \leq k$, to the vertex d_j of the graph G_n , which is defined in Section 2. Now the $k \times k$ vertex weighted Laplacian matrix $W(G_n)$ of G_n is given by

$$W(G_n) = \begin{bmatrix} M_{d_1} & -t_{1,2} & \dots & -t_{1,k} \\ -t_{2,1} & M_{d_2} & \dots & -t_{2,k} \\ \dots & \dots & \ddots & \dots \\ -t_{k,1} & -t_{k,2} & \dots & M_{d_k} \end{bmatrix},$$

where $M_{d_j} = \sum_{d_i \in N_{G_n}(d_j)} \phi(\frac{n}{d_i})$, for $1 \leq j \leq k$, and

$$t_{i,j} = \begin{cases} \phi(\frac{n}{d_j}) & \text{if } d_i \sim d_j \text{ in } G_n, \\ 0 & \text{otherwise,} \end{cases}$$

for $1 \leq i \neq j \leq k$.

In the following theorem, we determine the Laplacian spectrum of $\Gamma_2(\mathbb{Z}_n)$.

Theorem 3.3. *Let $d_1, d_2, \dots, d_k$ be the proper divisors of n . Then the Laplacian spectrum of $\Gamma_2(\mathbb{Z}_n)$ is given by*

$$\sigma_L(\Gamma_2(\mathbb{Z}_n)) = \left(\begin{array}{ccccc} 0 & M_{d_1} & M_{d_2} & \dots & M_{d_k} \\ 1 & \phi(\frac{n}{d_1}) - 1 & \phi(\frac{n}{d_2}) - 1 & \dots & \phi(\frac{n}{d_k}) - 1 \end{array} \right) \cup \sigma(W(G_n))$$

Proof. By Lemma 2.3, we have $\Gamma_2^*(\mathbb{Z}_n) = G_n[\overline{K}_{\phi(\frac{n}{d_1})}, \overline{K}_{\phi(\frac{n}{d_2})}, \dots, \overline{K}_{\phi(\frac{n}{d_k})}]$. Since the Laplacian eigenvalue of the graph $\overline{K}_m$ is 0 with multiplicity m , in view of Theorem 3.2, we have

$$\sigma_L(\Gamma_2^*(\mathbb{Z}_n)) = \left(\begin{array}{ccccc} M_{d_1} & M_{d_2} & \dots & M_{d_k} \\ \phi(\frac{n}{d_1}) - 1 & \phi(\frac{n}{d_2}) - 1 & \dots & \phi(\frac{n}{d_k}) - 1 \end{array} \right) \cup \sigma(W(G_n)).$$

Now, since $\Gamma_2(\mathbb{Z}_n) = K_1 \cup \Gamma_2^*(\mathbb{Z}_n)$, the result holds. $\square$

Note that since $\Gamma(\mathbb{Z}_n) = \Gamma_2(\mathbb{Z}_n) \vee K_{\phi(n)}$ and

$$\sigma_L(K_{\phi(n)}) = \left(\begin{array}{cc} 0 & \phi(n) \\ 1 & \phi(n) - 1 \end{array} \right),$$

by Theorems 3.1 and 3.3, in order to find the Laplacian spectrum $\Gamma(\mathbb{Z}_n)$, it is enough to determine $\sigma(W(G_n))$.

In the rest of this section, we discuss the Laplacian spectrum and Laplacian energy of $\Gamma(\mathbb{Z}_n)$, for (i) $n = p^t$, (ii) $n = pq$ and (iii) $n = p^2q$, where p and q are distinct prime numbers and t is a positive integer.

(i) Let $n = p^t$. Then since $\Gamma_2(\mathbb{Z}_{p^t})$ is an empty graph with $p^t - \phi(p^t) = p^{t-1}$ vertices, we have $\Gamma(\mathbb{Z}_{p^t}) = \overline{K}_{p^{t-1}} \vee K_{p^t - p^{t-1}}$.

Since

$$\sigma_L(\overline{K}_{p^{t-1}}) = \left(\begin{array}{c} 0 \\ p^{t-1} \end{array} \right) \text{ and } \sigma_L(K_{p^t - p^{t-1}}) = \left(\begin{array}{cc} 0 & p^t - p^{t-1} \\ 1 & p^t - p^{t-1} - 1 \end{array} \right),$$

it follows from Theorem 3.1 that

$$\sigma_L(\Gamma(\mathbb{Z}_{p^t})) = \left(\begin{array}{cccc} 0 & p^t - p^{t-1} & p^{t-1} & \\ 1 & p^{t-1} - 1 & 1 & p^t - p^{t-1} - 1 \end{array} \right).$$

Let m be the number of edges of $\Gamma(\mathbb{Z}_{p^t})$. Then we have

$$m = p^{t-1}(p^t - p^{t-1}) + \frac{(p^t - p^{t-1})(p^t - p^{t-1} - 1)}{2},$$

and so

$$\frac{2m}{p^t} = -p^{t-2} + p^t + p^{-1} - 1.$$

Therefore, the Laplacian energy of $\Gamma(\mathbb{Z}_{p^t})$ is determined by

$$\begin{aligned} LE(\Gamma(\mathbb{Z}_{p^t})) &= |p^{t-2} - p^t - p^{-1} + 1| + |p^{t-1} + p^{t-2} - p^t - p^{-1} + 1| \\ &+ (p^{t-1} - 1)|-p^{t-1} + p^{t-2} - p^{-1} + 1| + (p^t - p^{t-1} - 1)|p^{t-2} - p^{-1} + 1|. \end{aligned}$$

(ii) Let $n = pq$, where p and q are distinct prime numbers. Since the only proper divisors of n are p and q , the graph G_{pq} is $p \sim q$. By Lemma 2.3, we have

$$\Gamma(\mathbb{Z}_{pq}) = (K_1 \cup G_{pq}[\overline{K}_{\phi(q)}, \overline{K}_{\phi(p)}]) \vee K_{\phi(pq)}.$$

Since we have $M_p = \phi(\frac{n}{q}) = \phi(p) = p-1$ and $M_q = \phi(\frac{n}{p}) = \phi(q) = q-1$, it follows from Theorem 3.3 that

$$\begin{aligned} \sigma_L(\Gamma_2(\mathbb{Z}_{pq})) &= \begin{pmatrix} 0 & M_p & M_q \\ 1 & \phi(q) - 1 & \phi(p) - 1 \end{pmatrix} \cup \sigma(W(G_{pq})) \\ &= \begin{pmatrix} 0 & p-1 & q-1 \\ 1 & q-2 & p-2 \end{pmatrix} \cup \sigma(W(G_{pq})). \end{aligned}$$

Now, let $d_1 = p$ and $d_2 = q$. Then we have

$$W(G_{pq}) = \begin{bmatrix} \phi(p) & -\phi(p) \\ -\phi(q) & \phi(q) \end{bmatrix} = \begin{bmatrix} p-1 & 1-p \\ 1-q & q-1 \end{bmatrix}$$

with eigenvalues $p+q-2$ and 0 . Therefore

$$\sigma_L(\Gamma_2(\mathbb{Z}_{pq})) = \begin{pmatrix} 0 & p-1 & q-1 & p+q-2 \\ 2 & q-2 & p-2 & 1 \end{pmatrix}.$$

Since $\phi(pq) = pq - p - q + 1$ and $\Gamma(\mathbb{Z}_{pq})$ is the join of the graphs $\Gamma_2(\mathbb{Z}_{pq})$ and $K_{\phi(pq)}$, it follows from Theorem 3.1 that

$$\sigma_L(\Gamma(\mathbb{Z}_{pq})) = \begin{pmatrix} 0 & pq - p - q + 1 & pq - q & pq - p & p + q - 1 & pq \\ 1 & 2 & q - 2 & p - 2 & 1 & pq - p - q \end{pmatrix}.$$

The number of edges in $\Gamma(\mathbb{Z}_{pq})$ is equal to

$$m = (p-1)(q-1) + \frac{(pq-p-q+1)(pq-p-q)}{2} + (p+q-1)(pq-p-q+1)$$

and so

$$\frac{2m}{pq} = pq - 1 - pq^{-1} - qp^{-1} + q^{-1} + p^{-1}.$$

Now, the Laplacian energy of $\Gamma(\mathbb{Z}_{pq})$ is determined by $\sum_{i=1}^{pq} |\mu_i - \frac{2m}{pq}|$, where μ_i 's are the Laplacian eigenvalues of $\Gamma(\mathbb{Z}_{pq})$.

(iii) Let $n = p^2q$, where p and q are distinct prime numbers. Since p , q , and pq are the proper divisors of n , the graph G_{p^2q} is $p \sim q \sim p^2 \cup \{pq\}$. By Lemma 2.3, we have

$$\Gamma(\mathbb{Z}_{p^2q}) = (K_1 \cup G_{p^2q}[\overline{K}_{\phi(pq)}, \overline{K}_{\phi(p^2)}, \overline{K}_{\phi(q)}, \overline{K}_{\phi(p)}]) \vee K_{\phi(p^2q)}.$$

Also, we have

$$M_p = \phi\left(\frac{n}{p}\right) = \phi(p^2) = p^2 - p$$

$$M_q = \phi\left(\frac{n}{p}\right) + \phi\left(\frac{n}{p^2}\right) = \phi(pq) + \phi(q) = pq - p$$

$$M_{p^2} = \phi\left(\frac{n}{q}\right) = \phi(p^2) = p^2 - p$$

$$M_{pq} = 0.$$

Now, by Theorem 3.3, the Laplacian spectrum of $\Gamma_2(\mathbb{Z}_{p^2q})$ reads as follows:

$$\begin{aligned} \sigma_L(\Gamma_2(\mathbb{Z}_{p^2q})) &= \left(\begin{array}{ccccc} 0 & M_p & M_q & M_{p^2} & M_{pq} \\ 1 & \phi(pq) - 1 & \phi(p^2) - 1 & \phi(q) - 1 & \phi(p) - 1 \end{array} \right) \cup \sigma(W(G_{p^2q})) \\ &= \left(\begin{array}{cccc} 0 & p^2 - p & pq - p & \\ p - 1 & pq - p - 2 & p^2 - p - 1 & \end{array} \right) \cup \sigma(W(G_{p^2q})). \end{aligned}$$

Now, by taking $d_1 = p$, $d_2 = q$, $d_3 = p^2$, and $d_4 = pq$, we have

$$W(G_{p^2q}) = \begin{bmatrix} p^2 - p & -\phi(p^2) & 0 & 0 \\ -\phi(pq) & pq - p & -\phi(q) & 0 \\ 0 & -\phi(p^2) & p^2 - p & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix} = \begin{bmatrix} p^2 - p & -p^2 + p & 0 & 0 \\ -pq + p + q - 1 & pq - p & 1 - q & 0 \\ 0 & -p^2 + p & p^2 - p & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}$$

with

$$\sigma(W(G_{p^2q})) = \begin{pmatrix} 0 & p^2 - p & p(p+q-2) \\ 2 & 1 & 1 \end{pmatrix}.$$

Thus

$$\sigma_L(\Gamma_2(\mathbb{Z}_{p^2q})) = \begin{pmatrix} 0 & p^2 - p & pq - p & p^2 + pq - 2p \\ p+1 & pq - p - 1 & p^2 - p - 1 & 1 \end{pmatrix}.$$

Now, we have $\phi(p^2q) = p^2q - p^2 - pq + p$ and $\Gamma(\mathbb{Z}_{p^2q}) = \Gamma_2(\mathbb{Z}_{p^2q}) \vee K_{\phi(p^2q)}$. Hence, Theorem 3.1 implies that $\sigma_L(\Gamma(\mathbb{Z}_{p^2q}))$ is equal to

$$\begin{pmatrix} 0 & p^2q - p^2 - pq + p & p^2q - pq & p^2q - p^2 & p^2 + pq - p & p^2q \\ 1 & p+1 & pq - p - 1 & p^2 - p - 1 & 1 & p^2q - p^2 - pq + p - 1 \end{pmatrix}.$$

The number of edges in $\Gamma(\mathbb{Z}_{p^2q})$ is equal to

$$\begin{aligned} m = & (pq - p - q + 1)(p^2 - p) + (p^2 - p)(q - 1) \\ & + (p^2q - p^2 - pq + p)(p^2 + pq - p) \\ & + \frac{(p^2q - p^2 - pq + p)(p^2q - p^2 - pq + p - 1)}{2}, \end{aligned}$$

and also

$$\frac{2m}{p^2q} = \frac{p^3q^2 - p^3 + 2p - pq^2 - pq + q - 1}{pq}.$$

Now, the Laplacian energy of $\Gamma(\mathbb{Z}_{p^2q})$ can be determined by $\sum_{i=1}^{p^2q} |\mu_i - \frac{2m}{p^2q}|$, where μ_i 's are the Laplacian eigenvalues of $\Gamma(\mathbb{Z}_{p^2q})$.

4 Laplacian integrality, Algebraic connectivity and Laplacian spectral radius

Recall that a *decomposable graph* is one that can be constructed from isolated vertices by joins and unions.

By Lemma 2.3, we have that $\Gamma(\mathbb{Z}_n)$ is decomposable if and only if $\Gamma_2(\mathbb{Z}_n)$.

The following theorem, which is from [11], states a necessary and sufficient condition for a graph to be decomposable.

Theorem 4.1. [11, Theorem 2.5] *A graph is decomposable if and only if it does not have an induced subgraph isomorphic to P_4 .*

In the following theorem, we determine the decomposable comaximal graph of $\mathbb{Z}_n$.

Theorem 4.2. *The comaximal graph $\Gamma(\mathbb{Z}_n)$ is decomposable if and only if $n = p^\alpha q^\beta$, where p and q are prime numbers and α, β are nonnegative integers.*

Proof. First assume that $\Gamma(\mathbb{Z}_n)$ is decomposable. Let p, q and r be distinct proper divisors of n that are prime numbers. Then we have the induced subgraph $pq \sim r \sim p \sim qr$ of $\Gamma(\mathbb{Z}_n)$, which is isomorphic to P_4 . Hence Theorem 4.1 implies that $\Gamma(\mathbb{Z}_n)$ is not decomposable, which is impossible.

Now let $n = p^\alpha q^\beta$, where p and q are prime numbers and α, β are nonnegative integers. Assume on the contrary that $\Gamma(\mathbb{Z}_n)$ is not decomposable. Then by Theorem 4.1, it contains an induced subgraph $d_1 \sim d_2 \sim d_3 \sim d_4$ isomorphic to p_4 . Then we have $(d_1, d_3), (d_1, d_4), (d_2, d_4) \notin U(\mathbb{Z}_n)$ and $(d_1, d_2), (d_2, d_3), (d_3, d_4) \in U(\mathbb{Z}_n)$. Without loss of generality, assume that $p \mid (d_1, d_3)$. So if $p \mid (d_1, d_4)$, then $p \mid (d_3, d_4)$, which is impossible. So we have $q \mid (d_1, d_4)$. Now, if $p \mid (d_2, d_4)$, then we have that $p \mid (d_1, d_2)$, which is impossible. If $q \mid (d_2, d_4)$, then $q \mid (d_1, d_2)$, which is again impossible. So we should have $(d_2, d_4) = 1$, which is a contradiction with the fact that $(d_2, d_4) \notin U(\mathbb{Z}_n)$. $\square$

Recall that a graph G is *Laplacian integral* if all the Laplacian eigenvalues of G are integers. It follows from Theorem 3.1 that a decomposable graph is Laplacian integral.

The following two corollaries follow from Theorems 3.1, 3.3, and 4.2.

Corollary 4.3. *The comaximal graph $\Gamma(\mathbb{Z}_n)$ is Laplacian integral if and only if all the eigenvalues of $W(G_n)$ are integers.*

Corollary 4.4. *Let $n = p^\alpha q^\beta$, where p and q are prime numbers and α, β are nonnegative integers. Then $\Gamma(\mathbb{Z}_n)$ is Laplacian integral and so all the eigenvalues of $W(G_n)$ are integers.*

The *Laplacian spectral radius* of a graph G is defined as the largest Laplacian eigenvalue of G , and it is denoted by $\lambda(G)$.

In the following theorem, we recall a well-known bound for the Laplacian spectral radius of a graph.

Theorem 4.5. [6] *If G is a graph on n vertices, then $\lambda(G) \leq n$. Further, the equality holds if and only if $\overline{G}$ is disconnected if and only if G is the join of two graphs.*

In the next theorem, we determine the Laplacian spectral radius of $\Gamma(\mathbb{Z}_n)$.

Theorem 4.6. *In the comaximal graph of $\mathbb{Z}_n$, we have $\lambda(\Gamma(\mathbb{Z}_n)) = n$.*

Proof. By Lemma 2.3 and Theorem 4.5, the result holds. $\square$

The *algebraic connectivity* of G is the second smallest eigenvalue of $L(G)$ and it is denoted by $\mu(G)$. Also, the *vertex connectivity* of G , denoted by $\kappa(G)$, is the minimum number of vertices that are needed to be removed from $V(G)$ such that the induced subgraph of G on the remaining vertices is disconnected or has only one vertex. In [6], it was proved that $\mu(G) \leq \kappa(G)$ for a noncomplete graph G . For a complete graph K_n , it follows that $\mu(K_n) = n = \kappa(K_n) + 1$.

We use the following theorem to determine the algebraic connectivity and vertex connectivity of the comaximal graph $\Gamma(\mathbb{Z}_n)$.

Theorem 4.7. [7] *Let G be a noncomplete connected graph on n vertices. Then $\kappa(G) = \mu(G)$ if and only if G can be written as $G_1 \vee G_2$, where G_1 is a disconnected graph on $n - \kappa(G)$ vertices and G_2 is a graph on $\kappa(G)$ vertices with $\mu(G_2) \geq 2\kappa(G) - n$.*

Theorem 4.8. *In the comaximal graph of $\mathbb{Z}_n$, we have*

$$\mu(\Gamma(\mathbb{Z}_n)) = \phi(n) = \kappa(\Gamma(\mathbb{Z}_n)).$$

Proof. By Lemma 2.3, we have that

$$\Gamma(\mathbb{Z}_n) = H \vee K_{\phi(n)},$$

where the graph H has an isolated vertex. So $\kappa(\Gamma(\mathbb{Z}_n)) = \phi(n)$. Now, by Theorem 4.7, since H is a disconnected graph on $n - \phi(n)$ vertices, it is enough to show that $\mu(K_{\phi(n)}) \geq 2\kappa(\Gamma(\mathbb{Z}_n)) - n$. We have

$$\sigma_L(K_{\phi(n)}) = \begin{pmatrix} 0 & \phi(n) \\ 1 & \phi(n) - 1 \end{pmatrix},$$

and so $\mu(K_{\phi(n)}) = \phi(n)$. Since $\kappa(\Gamma(\mathbb{Z}_n)) = \phi(n)$, it is enough to show that $\phi(n) \geq 2\phi(n) - n$, or equivalently $n \geq \phi(n)$. Let $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_t^{\alpha_t}$ be the factorization of n to its prime powers, where $t, \alpha_1, \dots, \alpha_t$ are positive integers and $p_1, \dots, p_t$ are distinct prime numbers. Since $p_1 \dots p_t \geq (p_1 - 1) \dots (p_t - 1)$, we have $p_1^{\alpha_1} p_2^{\alpha_2} \dots p_t^{\alpha_t} \geq p_1^{\alpha_1 - 1} p_2^{\alpha_2 - 1} \dots p_t^{\alpha_t - 1} (p_1 - 1) \dots (p_t - 1)$.

Clearly $p_1^{\alpha_1-1} p_2^{\alpha_2-1} \dots p_t^{\alpha_t-1} (p_1 - 1) \dots (p_t - 1) = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_t^{\alpha_t} (1 - \frac{1}{p_1})(1 - \frac{1}{p_2}) \dots (1 - \frac{1}{p_t}) = \phi(n)$. Hence we have

$$\mu(\Gamma(\mathbb{Z}_n)) = \phi(n) = \kappa(\Gamma(\mathbb{Z}_n)).$$

□

Acknowledgements: The authors are deeply grateful to the referee for careful reading of the manuscript and helpful suggestions.

References

- [1] D. M. CARDOSO, M. A. A. DE FREITAS, E. A. MARTINS AND M. ROBBIANO, *Spectra of graphs obtained by a generalization of the join graph operation*, Discrete Math. **313** (2013) 733–741.
- [2] S. CHATTOPADHYAY, K. L. PATRA AND B. K. SAHOO, *Laplacian eigenvalues of the zero divisor graph of the ring $\mathbb{Z}_n$* , Linear Algebra Appl. **584** (2020) 267–286.
- [3] F. R. K. CHUNG, *Spectral Graph Theory*, AMS, 1997.
- [4] F. R. K. CHUNG AND R. P. LANGLANDS, *A combinatorial Laplacian with vertex weights*, J. Combin. Theory Ser. A **75** (1996) 316–327.
- [5] M. A. A. DE FREITAS, N. M. M. DE ABREU, R. R. DEL-VECCHIO AND S. JURKIEWICZ, *Infinite families of Q -integral graphs*, Linear Algebra Appl. **432** (2010) 2352–2360.
- [6] M. FIEDLER, *Algebraic connectivity of graphs*, Czechoslovak Math. J. **23** (1973) 298–305.
- [7] S. J. KIRKLAND, J. J. MOLITIERNO, M. NEUMANN AND B. L. SHADER, *On graphs with equal algebraic and vertex connectivity*, Linear Algebra Appl. **341** (2002) 45–56.
- [8] X. LIU AND P. LU, *Signless Laplacian spectral characterization of some joins*, Electron. J. Linear Algebra **30** (2015) 443–454.
- [9] H. R. MAIMANI, M. SALIMI, A. SATTARI AND S. YASSEMI, *Comaximal graph of commutative rings*, J. Algebra, **319** (2008) 1801–1808.

- [10] C. MCLEMAN AND E. MCNICHOLAS, *Spectra of coronae*, Linear Algebra Appl. **435** (2011) 998–1007.
- [11] R. MERRIS, *Laplacian graph eigenvectors*, Linear Algebra Appl. **278** (1998) 221–236.
- [12] B. MOHAR, *The Laplacian spectrum of graphs*, in - Graph Theory, Combinatorics, and Applications. Vol. 2 (Kalamazoo, MI, 1988), 871–898, Wiley-Intersci. Publ., Wiley, New York, 1991.
- [13] A. J. SCHWENK, *Computing the characteristic polynomial of a graph*, in - Graphs and Combinatorics, pp. 153–172, Lecture Notes in Math., Vol. 406 Springer, Berlin, 1974.
- [14] P. K. SHARMA AND S. M. BHATWADEKAR, *A note on graphical representation of rings*, J. Algebra **176** (1995) 124–127.
- [15] M. M. SLAVKO AND Z. Z. PETROVIC, *On the structure of comaximal graphs of commutative rings with identity*, Bull. Aust. Math. Soc. **83** (2011) 11–21.
- [16] H. J. WANG, *Graphs associated to co-maximal ideals of commutative rings*, J. Algebra **320** (2008) 2917–2933.
- [17] M. YOUNG, *Adjacency matrices of zero-divisor graphs of integers modulo n* , Involve **8** (2015) 753–761.

**THE NUMBER OF PRODUCTS OF N ELEMENTS
IN A NONASSOCIATIVE ALGEBRA**

Simon Davis

Research Foundation of Southern California
8861 Villa La Jolla Drive #13595
La Jolla, CA 92039

Received June 15, 2021

Revised June 21, 2021

Abstract

The ratio of the number of products of a N elements in an associative algebra converges to a limit as N increases. This limit determines the number of components required in a logic system once sequences with one more element are introduced.

1 Introduction

The Boolean logic of computers relies on a choice at each juncture such that it is not possible to reverse the route once that path has been taken. It follows that many algorithms depend on the order in which the operations are performed. Nonassociative algebras are characterized by the inequality of products evaluated in different orders. Therefore, the study of nonassociative algebras is relevant to the effectiveness of computational systems.

Consider an algebra that is not associative. The products of three elements depend on the order of evaluation. Therefore, there exist two different products of these elements defined by the order. This variety can be continued to a larger number of elements and the number of products can be determined. Given that each of these products is distinct, this number will be shown to be increasing by a multiplicative factor. As the number of elements, increases this number will be demonstrated to converge to a limit that will be evaluated. There are well known associative algebras where some of these products may be identified [1]. The conclusion concerning the number of products is relevant for the general nonassociative algebra without these identities.

2 The Number of Products of N Elements of a Nonassociative Algebra

Beginning with one or two elements, the uniqueness of the expression is evident. When there are three elements a , b and c , the products without any interchange of the order of these symbols are

$$(a \cdot b) \cdot c, a \cdot (b \cdot c). \quad (2.1)$$

The number of products of three elements then would equal 2.

Consider four elements, and the number of products derived from different orders of composition. It equals 5, with the list of combinations being

$$(a \cdot b) \cdot c \cdot d, (a \cdot (b \cdot c)) \cdot d, (a \cdot b) \cdot (cd), a \cdot ((b \cdot c) \cdot d), a \cdot (b \cdot (cd)). \quad (2.2)$$

For five elements, the products are

$$\begin{aligned} & (((a \cdot b)) \cdot d) \cdot e, ((a \cdot (b \cdot c)) \cdot d) \cdot e, ((a \cdot b) \cdot (cd)) \cdot e, (a \cdot ((b \cdot c) \cdot d)) \cdot e, \\ & (a \cdot (b \cdot (cd))) \cdot e, ((a \cdot b) \cdot (d \cdot e)), \\ & (a \cdot (b \cdot c)) \cdot (d \cdot e), (a \cdot b) \cdot ((cd) \cdot e), \\ & (a \cdot b) \cdot (c(d \cdot e)), a \cdot (((b \cdot c) \cdot d) \cdot e), a \cdot (((b \cdot (cd)) \cdot e), \\ & a \cdot ((b \cdot c) \cdot (d \cdot e)), a \cdot (b \cdot ((c \cdot d) \cdot e)), a \cdot (b \cdot (c \cdot (d \cdot e))). \end{aligned} \quad (2.3)$$

The products of an arbitrary number of elements also may be given. Let N be the number of symbols and $M(N)$ be the number of different products. Then

$$M(N) = \sum_{\substack{i+j=N \\ i,j \leq N-1}} M(i)M(j). \quad (2.4)$$

This number can be tabulated.

$\underline{N}$	$\underline{M(N)}$	
1	1	
2	1	
3	2	
4	5	
5	14	
6	42	
7	132	(2.5)
8	429	
9	1430	
10	4862	
11	16796	
12	58786	
13	208012	
14	742900	

The number $M(N)$ increases rapidly with N . A calculation of the ratios

$\frac{M(N+1)}{M(N)}$ also may be tabulated

N	$\frac{M(N+1)}{M(N)}$	
1	1	
2	2	
3	$2\frac{1}{2}$	
.. 4	$2\frac{4}{5}$	
5	3	
6	$3\frac{1}{7}$	
7	$3\frac{1}{4}$	(2.6)
8	$3\frac{1}{3}$	
9	$3\frac{2}{5}$	
10	$3\frac{5}{11}$	
11	$3\frac{1}{2}$	
12	$3\frac{7}{13}$	
13	$3\frac{4}{7}$	

The ratios have reduced denominators and the sequence is converging. Each value of $\frac{M(N+1)}{M(N)}$ for $5 \leq N \leq 13$ has the form $3 + \frac{N-5}{N+1}$.

3 The Limit of the Ratios of the Numbers of Products in a Nonassociative Algebra without Multiplicative Identities

The ratio of the number of products of $N+1$ elements to that for N elements in a nonassociative algebra that is not characterized by identities relating

the expressions is

$$\frac{M(N+1)}{M(N)} = \frac{\sum_{\substack{i+j=N+1 \\ i,j \leq N}} M(i)M(j)}{M(N)}. \quad (3.1)$$

Expanding the sum in the numerator

$$\begin{aligned} \frac{M(N+1)}{M(N)} &= \frac{M(1)M(N) + M(N)M(1)}{M(N)} + \sum_{\substack{i+j=N+1 \\ i,j \leq N-1}} \frac{M(i)M(j)}{M(N)} \\ &= 2 + \frac{M(2)M(N-1) + M(N-1)M(2)}{M(N)} + \sum_{\substack{i+j=N+1 \\ i,j \leq N-2}} \frac{M(i)M(j)}{M(N)} \\ &= 2 + 2\frac{M(N-1)}{M(N)} + 4\frac{M(N-2)}{M(N)} + 10\frac{M(N-3)}{M(N)} + \sum_{\substack{i+j=N+1 \\ i,j \leq N-5}} \frac{M(i)M(j)}{M(N)} \end{aligned} \quad (3.2)$$

The monotonicity of the function $\frac{M(N+1)}{M(N)}$ can be proven from this equation.

Theorem 3.1 The function $\frac{M(N+1)}{M(N)}$ is a monotonically increasing function of N .

Since $2\frac{M(N-1)}{M(N)} \leq \frac{2}{3}$ for $\frac{M(N)}{M(N-1)} \geq 3$, the other terms in the expression for $\frac{M(N+1)}{M(N)}$ then would sum to a number larger than $\frac{10}{3}$. When $\frac{M(N)}{M(N-1)}$ nearly equals 4, $2\frac{M(N-1)}{M(N)} \simeq \frac{1}{2}$, and the sum of the rest of the terms must equal nearly $\frac{7}{2}$.

Let $\frac{M(N)}{M(N-1)} = 4 - \varepsilon_0$, $\frac{M(N+1)}{M(N)} = 4 - \varepsilon_1$ and the sum of the rest of the terms be K . Then

$$\frac{M(N+1)}{M(N)} = K + 2\frac{M(N-1)}{M(N)} \quad (3.3)$$

and

$$4 - \varepsilon_1 = K + \frac{2}{4 - \varepsilon_0} \quad (3.4)$$

and

$$\begin{aligned}
 K &= 4 - \varepsilon_1 - \frac{2}{4 - \varepsilon_0} \\
 &= 4 - \varepsilon_1 - \frac{1}{2} \left(1 + \frac{\varepsilon_0}{4} + \frac{\varepsilon_0^2}{4^2} + \dots \right) \\
 &= \frac{7}{2} - \varepsilon_1 - \frac{\varepsilon_0}{8} - \frac{\varepsilon_0^2}{32} - \dots
 \end{aligned} \tag{3.5}$$

Then

$$\begin{aligned}
 &\frac{M(N)}{M(N-1)} \left(\frac{M(N)}{M(N-1)} - K - 2 \frac{M(N-1)}{M(N)} \right) \\
 &= \left(\frac{M(N)}{M(N-1)} \right)^2 - K \left(\frac{M(N)}{M(N-1)} \right) - 2 \\
 &= (4 - \varepsilon_0)^2 - \left(\frac{7}{2} - \varepsilon_1 - \frac{\varepsilon_0}{8} - \frac{\varepsilon_0^2}{32} - \dots \right) (4 - \varepsilon_0) - 2 \\
 &= 16 - 8\varepsilon_0 + \varepsilon_0^2 - 14 + 4\varepsilon_1 + \frac{\varepsilon_0}{2} + \frac{\varepsilon_0^2}{8} \\
 &\quad + \dots + \frac{7}{2}\varepsilon_0 - \varepsilon_0\varepsilon_1 - \frac{\varepsilon_0^2}{8} - \dots - 2 \\
 &= -4\varepsilon_0 + 4\varepsilon_1 + \varepsilon_0^2 - \varepsilon_1
 \end{aligned} \tag{3.6}$$

which equals zero if $\varepsilon_0 = \varepsilon_1$. Substitution into K gives

$$K(\varepsilon_1 = \varepsilon_0) = \frac{7}{2} - \frac{9}{8}\varepsilon_0 - \frac{\varepsilon_0^2}{32} - \dots \tag{3.7}$$

while the upper root to the quadratic equation

$$\left(\frac{M(N)}{M(N-1)} \right)^2 - K \left(\frac{M(N)}{M(N-1)} \right) - 2 = 0 \tag{3.8}$$

equals

$$\begin{aligned}
 \frac{K + (K^2 + 8)^{\frac{1}{2}}}{2} &= \frac{7}{4} - \frac{9}{16}\varepsilon - \frac{\varepsilon_0^2}{64} - \dots + \frac{1}{2} \left[\frac{81}{4} - \frac{9}{4}\varepsilon_0 - \frac{67}{64}\varepsilon_0^2 - \dots \right]^{\frac{1}{2}} \\
 &= 4 - \frac{11}{16}\varepsilon_0 + \dots
 \end{aligned} \tag{3.9}$$

which is a contradiction by yielding a value of $\frac{M(N)}{M(N-1)}$ larger than $\frac{M(N+1)}{M(N)}$. It is necessary, therefore, to restore consistency by requiring $\frac{M(N+1)}{M(N)} > \frac{M(N)}{M(N-1)}$.

The terms in the sum are characterized by factors $M(i)$ such that $\frac{M(i+1)}{M(i)} \geq 3$. with the coefficients increasing faster than a power of 3, an upper bound for the expansion in Eq.(3.2) does not exist if the lower bound for $\frac{M(N)}{M(N-1)}$ is chosen to be 3. For example, if one sets $3 \leq \frac{M(i+1)}{M(i)} \leq 4$ for $5 \leq i \leq N-1$, it is found that

$$\frac{3}{4} \leq \frac{M(i)}{M(i+1)} \frac{M(N+1-i)}{M(N-i)} \leq \frac{4}{3} \quad (3.10)$$

and

$$\frac{M(i)}{M(i+1)} \frac{M(N-4)}{M(N-5)} \geq 1. \quad (3.11)$$

The upper bound is

$$\sum_{\substack{i+j=N+1 \\ i,j \leq N-5}} \frac{M(i)M(j)}{M(N)} \leq 2(N-8) \frac{M(5)M(N-4)}{M(N)} \quad (3.12)$$

which increases with N .

The bound can be reduced with a formula for $\frac{M(i+1)}{M(i)}$ for $iN-1$.

Theorem 3.2 The limiting value of the ratio $\frac{M(N+1)}{M(N)}$ satisfies the inequality

$$3.671875 \leq \frac{M(N+1)}{M(N)} \leq 4.25386149308. \quad (3.13)$$

Proof. From §2, it had been found that $\frac{M(i+1)}{M(i)} = 3 + \frac{i-5}{i-1}$ for $5 \leq i \leq 13$. Let $\frac{M(i+1)}{M(i)} = 3 + \frac{i-5}{i+1}$ for $5 \leq i \leq N-1$. Provided this form of the ratio is

valid for sufficiently large N , the inequality can be proven. Then

$$\begin{aligned} \frac{M(N+1)}{M(N)} &= 2 + \frac{2}{3 + \frac{N-6}{N}} + \frac{4}{\left(3 + \frac{N-6}{N}\right) \left(3 + \frac{N-7}{N-1}\right)} \\ &+ \frac{10}{\left(3 + \frac{N-6}{N}\right) \left(3 + \frac{N-7}{N-1}\right) \left(3 + \frac{N-8}{N-2}\right)} \\ &+ \frac{28}{\left(3 + \frac{N-6}{N}\right) \left(3 + \frac{N-7}{N-1}\right) \left(3 + \frac{N-8}{N-2}\right) \left(3 + \frac{N-9}{N-3}\right)} \\ &\quad \left[1 + 2 \sum_{i'=6}^{\lfloor \frac{N-4}{2} \rfloor} \prod_{i=6}^{i'} \frac{3 + \frac{i-5}{i+1}}{3 + \frac{N-4-i}{N+1-i}} \right]. \end{aligned} \quad (3.14)$$

The limit as N tends to infinity is

$$\lim_{N \rightarrow \infty} \frac{M(N+1)}{M(N)} = 2 + \frac{2}{4} + \frac{10}{4^3} + \frac{28}{4^4} \left(1 + 2 \sum_{i'=6}^{\frac{3 + \frac{i-5}{i+1}}{4}} \right). \quad (3.15)$$

The product in the last term satisfies the inequality

$$\left(\frac{3}{4} \right)^k \prod_{i=6}^{i'} \frac{3 + \frac{i-5}{i+1}}{4} < e^{\frac{1}{8}} \left(\frac{3}{4} e^{\frac{1}{8}} \right)^k \quad (3.16)$$

$k = i' - 5$

because the remainder larger than $\frac{3}{4}$ changes by increments that can be approximated by an even distribution, yielding

$$x^k \left(1 + \frac{\alpha}{x} \right) \dots \left(1 + \frac{kx}{\alpha} \right) \quad (3.17)$$

where $x = \frac{3}{4}$, $\frac{kx}{\alpha} \leq \frac{1}{4}$, and

$$\begin{aligned} \left(1 + \frac{\alpha}{x} \right) \dots \left(1 + \frac{k\alpha}{x} \right) &< \exp \left(\sum_{\ell=1}^k \frac{\ell\alpha}{x} \right) = \exp \left(\frac{k(k+1)}{2} \frac{\alpha}{x} \right) \\ &\leq \exp \left(\frac{k+1}{8} \right). \end{aligned} \quad (3.18)$$

Substituting the bounds into the sum,

$$\begin{aligned} 2.90625 + \frac{28}{4^4} \left(1 + 2 \sum_{k=1}^{\infty} \left(\frac{3}{4} \right)^k \right) &< \lim_{N \rightarrow \infty} \frac{M(N+1)}{M(N)} \\ &< 2.90625 + \frac{28}{4^4} \left(1 + 2e^{\frac{1}{8}} \sum_{k=1}^{\infty} \left(\frac{3}{4} e^{\frac{1}{8}} \right)^k \right) \end{aligned} \quad (3.19)$$

or

$$3.671875 < \frac{M(N+1)}{M(N)} < 4.25386149308. \quad (3.20)$$

The condition $\frac{M(i+1)}{M(i)} = 3 + \frac{i-5}{i+1}$, for $5 \leq i \leq N-1$ and sufficiently large values of N , was required for the proof of this inequality. For sufficiently large values of N , the product will be restricted within the required range because the higher terms are infinitesimal.

An arithmetic identity is required to prove that the limit of the ratio as $i \rightarrow \infty$ is 4. By Eq.(3.13),

$$\lim_{N \rightarrow \infty} = 2 + \frac{2}{4} + \frac{4}{16} + \frac{5}{32} + \frac{28}{256} \lim_{N \rightarrow \infty} \left[1 + 2 \sum_{i' \geq 6}^{\lfloor \frac{N_4}{2} \rfloor} \prod_{i=6}^i \frac{3 + \frac{i-5}{i+1}}{3 + \frac{N-4-i}{N-i-1}} \right] \quad (3.21)$$

Setting the limit to be tending to 4,

$$4 \doteq 2 + \frac{1}{2} + \frac{1}{4} + \frac{5}{32} + \frac{7}{64} \lim_{N \rightarrow \infty} \left[1 + 2 \sum_{i' \geq 6}^{\lfloor \frac{N_4}{2} \rfloor} \prod_{i=6}^i \frac{3 + \frac{i-5}{i+1}}{3 + \frac{N-4-i}{N-i-1}} \right], \quad (3.22)$$

$$\frac{35}{32} \doteq \frac{7}{64} \lim_{N \rightarrow \infty} \left[1 + 2 \sum_{i' \geq 6}^{\lfloor \frac{N_4}{2} \rfloor} \prod_{i=6}^i \frac{3 + \frac{i-5}{i+1}}{3 + \frac{N-4-i}{N-i-1}} \right], \quad (3.23)$$

and

$$10 \doteq \lim_{N \rightarrow \infty} \left[1 + 2 \sum_{i' \geq 6}^{\lfloor \frac{N_4}{2} \rfloor} \prod_{i=6}^i \frac{3 + \frac{i-5}{i+1}}{3 + \frac{N-4-i}{N-i-1}} \right]. \quad (3.24)$$

4 General Formula for the Number of Nonassociative Products

The grouping of terms in a product with n factors has been found to be given by a formula which is valid also for several other problems such as the computation of the number of stairways paths from $(0, 0)$ to (N, N) underneath the diagonal and the number of partitions of polygons by nonintersecting diagonals into triangles [2]. The number of nonassociative products of n terms with k elements preceding the rightmost left parenthesis is $F(N, k)$, which satisfies the recursion relation $F(N, k) = F(N-1, k) + F(N-1, k-1)$, which can be solved by $F(N, k) = \binom{N+k-2}{k} - \binom{N+k-1}{k-1}$. The total number of nonassociative products with N factors is

$$F(N) = \sum_{j=0}^{N-2} F(N, j) = \frac{(2N-2)!}{N!(N-1)!} \quad (4.1)$$

which equals C_{N-1} , where $C_N = \frac{\binom{2N}{N}}{N+1} = \frac{(2N)!}{(N+1)N!}$ is the Catalan number. Given this formula, the limit of the ratio in Section 3 may be evaluated to be

$$\lim_{N \rightarrow \infty} \frac{F(N+1)}{F(N)} = \lim_{N \rightarrow \infty} \frac{2^{2N}}{2^{2N-2}} \frac{N-1}{N} \sqrt{\frac{N}{N+1}} = \lim_{N \rightarrow \infty} 4 \frac{N-1}{N} \sqrt{\frac{N}{N+1}} = 4. \quad (4.2)$$

The limiting value of 4 has been found again for this ratio. Consequently, the number of choices in a computer algorithm for listing the nonassociative products of N terms increases by a factor of 4 for large N without any additional conditions.

There may be nontrivial identities in an algebra which would affect this counting. A method for establishing identities in a nonassociative algebra has been given by considering the space of homogeneous multilinear monomials of degree N and then reducing the number of linearly independent

rows [3]. A non-zero null space would represent the existence of identities in the algebra.

Now consider the octonion algebra with basis elements $e_0, e_1, \dots, e_7$, where $e_0^2 = 1$, $e_i^2 = -1$, $e_0 e_i = e_i e_0$ and $e_i e_j = f_{ijk} e_k$, $i, j, k = 1, \dots, 7$, with f_{ijk} being the structure constants. Amongst these elements there exist triples which form quaternion subalgebras. Furthermore, there are multiplication rules of an alternative algebra

$$\begin{aligned}(xy)x &= x(yx) \\ x(xy) &= x^2 y \\ (xy)y &= xy^2\end{aligned}\tag{4.3}$$

and the Moufang identities [1]

$$\begin{aligned}(ax)(ya) &= a((xy)a) \\ a(x(ay)) &= (a(xa))y \\ x(a(ya)) &= ((xa)y)a.\end{aligned}\tag{4.4}$$

The problem of counting the number of different nonassociative products in an octonion algebra now may be considered.

Suppose that two out of three of the elements in a product are identical. Then, the laws of an alternative algebra will determine equivalency classes. This effect could occur, for example, with quarks in the protons and neutrons. Since there are two up quarks and one quarks in a proton and two down quarks and one up quark form a neutron, matter composed of protons or neutrons would have 2/3 of the quarks identical. The conglomeration of protons does not have electrical stability, and, therefore, it is sufficient to consider only compound states of neutrons. A typical product consisting of two types of factors would be $xyxyx.yxx\dots$ with $3n$ elements. Initially, the number of groupings equals

$$C_{3n-1} = \frac{(6n-2)!}{(3n-1)!((3n)!)}. \tag{4.5}$$

By the rules of alternativity, the parentheses with an group of three elements can be placed anywhere in a triple.

Denoting the number of independent products to be G_N , $N = 3n$ the enumeration is

$$N = 3 : xxy = x(xy) = x^2y \quad G_3 = 1$$

$$N = 6 : xxyyxx \quad G_6 = 39$$

$$\begin{aligned} & (((((x \cdot x) \cdot y) \cdot y) \cdot x) \cdot x) \\ & (((((x \cdot x) \cdot y) \cdot (y \cdot x)) \cdot x) \\ & (((((x \cdot x) \cdot (y \cdot y)) \cdot x) \cdot x)) \\ & (((((x \cdot x) \cdot ((y \cdot y) \cdot x)) \cdot x) \\ & (((((x \cdot x) \cdot (y \cdot (y \cdot x))) \cdot x) \\ & (((((x \cdot (x \cdot y)) \cdot y) \cdot x) \cdot x) \\ & (((((x \cdot (x \cdot y)) \cdot (y \cdot x)) \cdot x) \\ & (((((x \cdot ((x \cdot y) \cdot y)) \cdot x) \cdot x) \\ & (((((x \cdot (x \cdot (y \cdot y))) \cdot x) \cdot x) \\ & (((((x \cdot ((x \cdot y) \cdot y) \cdot x)) \cdot x) \\ & ((x \cdot (x \cdot y)) \cdot (y \cdot (x \cdot x))) \\ & ((x \cdot ((x \cdot y) \cdot (y \cdot x))) \cdot x) \\ & ((x \cdot ((x \cdot (y \cdot y)) \cdot x)) \cdot x) \\ & ((x \cdot ((x \cdot (y \cdot y)) \cdot x))) \cdot x) \\ & (((((x \cdot x) \cdot y) \cdot y) \cdot (x \cdot x) \\ & (((((x \cdot x) \cdot y) \cdot ((y \cdot x) \cdot x)) \\ & (((((x \cdot x) \cdot (y \cdot y))) \cdot (x \cdot x) \\ & ((x \cdot x) \cdot ((y \cdot y) \cdot x)) \cdot x) \\ & ((x \cdot (x \cdot y)) \cdot y) \cdot (x \cdot x) \end{aligned}$$

$$\begin{aligned}
& (x \cdot (x \cdot y)) \cdot ((y \cdot x) \cdot x) \\
& (x \cdot (x \cdot (y \cdot y))) \cdot (x \cdot x) \\
& (x \cdot ((x \cdot y) \cdot y)) \cdot (x \cdot x) \\
& ((x \cdot x) \cdot y) \cdot ((y \cdot x) \cdot x) \\
& (x \cdot ((x \cdot (y \cdot y)) \cdot (x \cdot x))) \\
& (x \cdot x) \cdot (y \cdot (y \cdot x)) \cdot x \\
& (x \cdot (((x \cdot y) \cdot y) \cdot x) \cdot x) \\
& (x \cdot ((x \cdot ((y \cdot y) \cdot x)) \cdot x)) \\
& (x \cdot ((x \cdot (y \cdot (y \cdot x)))) \cdot x) \\
& ((x \cdot x) \cdot y) \cdot (y \cdot (x \cdot x)) \\
& ((x \cdot x) \cdot (y \cdot (y \cdot x) \cdot x)) \\
& ((x \cdot x) \cdot ((y \cdot y) \cdot (x \cdot x))) \tag{4.6} \\
& (x \cdot x) \cdot ((y \cdot y) \cdot x) \cdot x \\
& (x \cdot x) \cdot ((y \cdot (y \cdot x)) \cdot x) \\
& (x \cdot (x \cdot y)) \cdot (y \cdot (x \cdot y)) \\
& (x \cdot (((x \cdot y) \cdot y)) \cdot x) \cdot x) \\
& (x \cdot (((x \cdot (y \cdot y)) \cdot x) \cdot x)) \\
& (x \cdot ((x \cdot (y \cdot y)) \cdot (x \cdot x))) \\
& (x \cdot (((x \cdot y) \cdot (y \cdot x)) \cdot x)) \\
& (x \cdot (((x \cdot (y \cdot y)) \cdot x) \cdot x)) \\
& (x \cdot ((x \cdot (y \cdot y)) \cdot x) \cdot x)) \\
& (x \cdot ((x \cdot ((y \cdot y) \cdot x)) \cdot x)) \\
& (x \cdot ((x \cdot (y \cdot (y \cdot x)))) \cdot x))
\end{aligned}$$

The only identifications could be made within separate triples such that $((x \cdot x) \cdot y) \cdot ((y \cdot x) \cdot x) = (x \cdot (x \cdot y)) \cdot (y \cdot (x \cdot x)) = ((x \cdot x) \cdot y) \cdot (y \cdot (x \cdot x)) = (x \cdot (x \cdot y)) \cdot (y \cdot (x \cdot x))$.

More generally, there will be 2^n identifications in a set of n triples, and

$$G_{3n} = C_{3n-1} - 2^n - 1. \quad (4.7)$$

Consequently, the ratios $\frac{G_{3(n+1)}}{G_{3n}}$ are given by

$$\frac{G_{3(n+1)}}{G_{3n}} = \frac{C_{3n+2} - 2^{n+1} - 1}{C_{3n-1} - 2^n - 1}. \quad (4.8)$$

The Catalan numbers equal

$$\begin{aligned} C_{3n-1} &\simeq \frac{1}{\sqrt{2\pi e}} 2^{6n-2} \left(\frac{3n-1}{3n} \right)^{3n} \frac{1}{3n-1} \sqrt{\frac{2}{3n}} \\ C_{3n+2} &\simeq \frac{1}{\sqrt{2\pi e}} 2^{6n+4} \left(\frac{3n+2}{3n+3} \right)^{3(n+1)} \frac{1}{3n+2} \sqrt{\frac{2}{3(n+1)}}. \end{aligned} \quad (4.9)$$

for large n .

Then

$$\begin{aligned} &\lim_{n \rightarrow \infty} \frac{G_{3(n+1)}}{G_{3n}} \\ &\simeq \lim_{n \rightarrow \infty} \frac{\frac{1}{\sqrt{2\pi e}} 2^{6n+4} \left(\frac{3n+2}{3n+3} \right)^{3(n+1)} \frac{1}{3n+2} \sqrt{\frac{2}{3(n+1)}} - 2^{n+1} - 1}{\frac{1}{\sqrt{2\pi e}} 2^{6n-2} \left(\frac{3n-1}{3n} \right)^{3n} \frac{1}{3n-1} \sqrt{\frac{2}{3n}} - 2^n - 1} \\ &\simeq \lim_{n \rightarrow \infty} \frac{2^6 \left(1 - \frac{1}{3n}\right)^3 \left(1 - \frac{1}{n}\right)^{\frac{3}{2}} - \sqrt{\pi e} \left(1 - \frac{1}{3n}\right)^{-3n} (3n)^{\frac{3}{2}} 2^{-5n+4}}{1 - \sqrt{\pi e} \left(1 - \frac{1}{3n}\right)^{-3n} (3n)^{\frac{3}{2}} 2^{-5n+2}} \\ &= \lim_{n \rightarrow \infty} 2^6 \left(1 - \frac{5}{2n} + \mathcal{O}\left(\frac{1}{n^2}\right) \right) \\ &= 2^6. \end{aligned} \quad (4.10)$$

5 Nonassociativity and The Hadronic Spectrum

Given that the quarks belong to an octonion module, an increase in the number of resonances of compound neutron states can be predicted theoretically. Similarly, with three different quarks, the number of products of elements, which can be grouped into multiples of four, would be decreased by the Moufang identities.

Every baryon in the $\frac{1}{2}^+$ octet, except Σ^0 and Λ^0 , is the combination of two quarks of one kind and one of another type or three identical quarks. These configurations would be associative groupings by left and right alternativity

$$x^2y = x(xy) \quad yx^2 = (yx)x. \quad (5.1)$$

However, the state uds either can be $(ud)s$ or $u(ds)$ and describes the quark content of Σ^0 and Λ^0 . Therefore, the mass difference would be a physical effect of the associator

$$[u, d, s] = (ud)s - u(ds). \quad (5.2)$$

Similarly, the nine of the baryons in the $\frac{3}{2}^+$ decuplet are composite states that are associative groups. The remaining baryon Σ^{*0} is an excited state of uds .

With the charm quark, the $\frac{1}{2}^+$ baryons form a tetrahedron. Four of the six elements on the second level and all on the third level have a minimum of two quarks of one type. Only $\Xi_c^0 = dsc$ and $\Xi_c^+ = usc$ have three different quarks. In the pyramid of $\frac{3}{2}^+$ states, there are only three more baryons, $\Xi_c^{*0} = dsc$, $\Xi_c^{*+} = usc$ and $\Sigma_c^{*+} = udc$, which are composed of different quarks. Altogether, 13 of 17 elements in the $\frac{1}{2}^+$ tetrahedron and 15 of 19 baryons in the $\frac{3}{2}^+$ pyramid have an associative grouping of quarks.

The rest masses of the anomalous baryons [4] is given:

$$\begin{aligned}
m^{\Lambda^0} &= 1115.6830.006 \text{ MeV}/c^2 \\
m_{\Sigma^0} &= 1192.642 \pm 0.024 \text{ MeV}/c^2 \\
m_{\Sigma^+0} &= 1383.7 \pm 1.0 \text{ MeV}/c^2 \\
m_{\Xi_c^+} &= 2467.8^{+0.4}_{-0.6} \text{ MeV}/c^2 \\
m_{\Xi_c^0} &= 2470.88^{+0.34}_{-0.80} \text{ MeV}/c^2 \\
m_{\Sigma_c^{*+}} &= 2517.5 \pm 2.3 \text{ MeV}/c^2 \\
m_{\Xi_c^{*+}} &= 2575.6 \pm 3.1 \text{ MeV}/c^2 \\
m_{\Xi_c^{*0}} &= 2577.9 \pm 2.9 \text{ MeV}/c^2.
\end{aligned} \tag{5.3}$$

The difference between m_{Σ^0} and m_{Λ^0} then equals $(76.959 \pm 0.003) \text{ MeV}/c^2$ even though these two baryons consist of the same quarks. The different isospin does not affect the spin coupling formula

$$m_{q_1 q_2 q_3} = m_1 + m_2 + m_3 + A' \left(\frac{\vec{S}_1 \cdot \vec{S}_2}{m_1 m_2} + \frac{\vec{S}_1 \cdot \vec{S}_3}{m_1 m_3} + \frac{\vec{S}_2 \cdot \vec{S}_3}{m_2 m_3} \right) \tag{5.4}$$

The values of the quark masses have been selected in the literature to be $362 \text{ MeV}/c^2$, $366 \text{ MeV}/c^2$ and $537 \text{ MeV}/c^2$ for m_u, m_d and m_s . An estimate of A' has been given, based on the following argument for equal masses. Supposes that the masses of the quarks in the baryon are nearly equal. Then

$$m_{q_1 q_2 q_3} \simeq 3m_1 + A' \sum_{i < j} \frac{\vec{S}_i \cdot \vec{S}_j}{m_1^2}. \tag{5.5}$$

Since $\vec{S}^2 = (\vec{S}_1 + \vec{S}_2 + \vec{S}_3)^2 = \vec{S}_1^2 + \vec{S}_2^2 + \vec{S}_3^2 + 2 \sum_{i < j} \vec{S}_i \cdot \vec{S}_j$,

$$2 \sum_{i < j} \vec{S}_i \cdot \vec{S}_j = \vec{S}^2 - (\vec{S}_1^2 + \vec{S}_2^2 + \vec{S}_3^2) \tag{5.6}$$

However, since the eigenvalues of $\vec{S}^2$ are $S(S+1)$ for a spin operator, it is not possible to deduce the sum of the inner products from this formula. The result, $-\frac{3}{4}$, will be demonstrated to be invalid for the physical configuration with a total spin of $\frac{1}{2}$.

It is evident that $\vec{S}_i \cdot \vec{S}_j$ either equals $\frac{1}{4}$ or $-\frac{1}{4}$ if the spins are aligned in the same direction or point in opposite directions respectively. There are only two kinds of arrangements of spins for a composite system of three quarks. Either two or three spins are aligned. The total spin equals $\frac{1}{2}$ or $\frac{3}{2}$ respectively. Then, for the $\frac{1}{2}^+$ octet of baryons, two pairs will be pointing in opposite directions and one pair will be parallel, yielding

$$\sum_{i < j} \vec{S}_i \cdot \vec{S}_j = -\frac{1}{4}. \quad (5.7)$$

Consequently, the formula for equal quark masses must be

$$m_{q_1 q_2 q_3} \simeq 3m_1 - \frac{A'}{4} \frac{1}{m_1^2} \quad m_1 \approx m_2 \approx m_3 \quad (5.8)$$

The relation used in the literature, with a factor of $\frac{3A'}{4}$, is based on a value of $0.026 \left(\frac{GeV}{c^2}\right)^3$ for A' . Since the formula is demonstrated to have a factor of only $\frac{A'}{4}$, the factor of 3 may be absorbed into A' . Then, the masses of $\frac{1}{2}^+$ baryons can be calculated through Eq.(4.14) with $A' = 0.078 \left(\frac{GeV}{c^2}\right)^3$.

Interchanging the signs of the inner products of the spin vectors, there are three possible values of baryon masses

$$\begin{aligned} m_{q_1 q_2 q_3}^{(1)} &= m_1 + m_2 + m_3 + \frac{A'}{4} \left(\frac{1}{m_1 m_2} - \frac{1}{m_1 m_3} - \frac{1}{m_2 m_3} \right) \\ m_{q_1 q_2 q_3}^{(2)} &= m_1 + m_2 + m_3 + \frac{A'}{4} \left(-\frac{1}{m_1 m_2} + \frac{1}{m_1 m_3} - \frac{1}{m_2 m_3} \right) \\ m_{q_1 q_2 q_3}^{(3)} &= m_1 + m_2 + m_3 + \frac{A'}{4} \left(-\frac{1}{m_1 m_2} - \frac{1}{m_1 m_3} + \frac{1}{m_2 m_3} \right) \end{aligned} \quad (5.9)$$

For the uds state,

$$\begin{aligned} m_{uds}^{(1)} &= 1212.65 \text{ MeV}/c^2 \\ m_{uds}^{(2)} &= 1118.918 \text{ MeV}/c^2 \\ m_{uds}^{(3)} &= 1116.725 \text{ MeV}/c^2. \end{aligned} \quad (5.10)$$

The mass $m_{uds}^{(1)}$ differs from m_{Σ^0} by almost $20 \text{ MeV}/c^2$ and $m_{uds}^{(3)}$ is nearly equal to m_{Λ^0} . It will not be possible to adjust the error in $m_{uds}^{(1)}$ without affecting $m_{uds}^{(3)}$. Nevertheless, there exist values of m_u , m_d , m_s and A' . Let

$$\begin{aligned} (m_u + m_d + m_s) + \frac{A'}{4}(-2.65453719507 \text{ GeV}/c^2)^{-2} &\simeq 1.119265 \text{ GeV}/c^2 \\ (m_u + m_d + m_s) + \frac{A'}{4}(-7.603342 \text{ GeV}/c^2)^{-2} &\simeq 1.11583 \text{ GeV}/c^2. \end{aligned} \quad (5.11)$$

Subtracting the second equation from the first gives

$$\frac{A'}{4}(4.9193048149 \text{ GeV}/c^2) \simeq 0.07682 \text{ GeV}/c^2 \quad (5.12)$$

and

$$A'_m \simeq 0.06246110593 (\text{GeV}/c^2)^3 \quad (5.13)$$

required for the theoretical prediction of the two baryon masses. Then

$$m_u + m_d + m_s \simeq 1234.5718069 \text{ MeV}/c^2. \quad (5.14)$$

Specifying that $m_d = m_u + 4 \text{ MeV}/c^2$ and altering the masses from the values given after Eq.(5.4) by the same amount Δm ,

$$\begin{aligned} 2m_u + m_s &\simeq 1230.5718069 \text{ MeV}/c^2 \\ 2(m_u + \Delta m) + (m_s + \Delta m) &= 1265 \text{ MeV}/c^2. \end{aligned} \quad (5.15)$$

Then

$$\Delta m \simeq 11.476064635 \text{ MeV}/c^2. \quad (5.16)$$

and the quark masses may be set equal to

$$\begin{aligned} m_u^{not \text{ weighted}} &\simeq 350.52393564 \text{ MeV}/c^2 \\ m_d^{not \text{ weighted}} &\simeq 354.52393564 \text{ MeV}/c^2 \\ m_s^{not \text{ weighted}} &\simeq 525.52393564 \text{ MeV}/c^2. \end{aligned} \quad (5.17)$$

to match the experimental measurements. The u and d spins are aligned in $m_{uds}^{(1)}$, while the d and s spins are parallel in $m_{uds}^{(3)}$. It follows that $(ud)s$ would be identified with a primary interaction of u and d spins and Σ^0 , whereas $u(ds)$ is a configuration, with a coupling between parallel d and s spins, that can be regarded as the Λ^0 baryon. Recalling the wavefunction for a baryon may be constructed from by tensoring symmetric two-quark states with a single quark state. When it has total spin $\frac{1}{2}$,

$$\begin{aligned} \left| \frac{1}{2}, \frac{1}{2} \right\rangle &= \frac{1}{\sqrt{6}} (2 \uparrow\uparrow\downarrow - \uparrow\downarrow\uparrow - \downarrow\uparrow\uparrow) \\ \left| \frac{1}{2}, -\frac{1}{2} \right\rangle &= \frac{1}{\sqrt{6}} (2 \downarrow\downarrow\uparrow - \downarrow\uparrow\downarrow - \uparrow\downarrow\downarrow). \end{aligned} \tag{5.18}$$

The wavefunctions are symmetric with respect to the spins of the first two quarks. However, the interchange with the spin of the third quark alters the above states. For example, the interchange of the second and third spins in $\left| \frac{1}{2}, \frac{1}{2} \right\rangle$ gives $\frac{1}{\sqrt{6}} (2 \uparrow\downarrow\uparrow - \uparrow\uparrow\downarrow - \downarrow\uparrow\uparrow)$ which has an inner product equal only to $\frac{2}{3}$ with $\left| \frac{1}{2}, \frac{1}{2} \right\rangle$.

With the weighting in these quantum states, the linear combination of the squared magnitudes of the coefficients must be inserted into the spin

coupling mass formula. Therefore, using the data

$$\begin{aligned}
 m_{(ud)s} &= \frac{2}{3}m_{uds}^{(1)} + \frac{1}{6}m_{uds}^{(2)} + \frac{1}{6}m_{uds}^{(3)} \\
 &= \frac{2}{3}(1212.65 \text{ MeV}/c^2) + \frac{1}{6}(1118.918 \text{ MeV}/c^2) \\
 &\quad + \frac{1}{6}(1116.725 \text{ MeV}/c^2) \\
 &= 1181.0405 \text{ MeV}/c^2 \\
 m_{u(ds)} &= \frac{1}{6}m_{uds}^{(1)} + \frac{1}{6}m_{uds}^{(2)} + \frac{2}{3}m_{uds}^{(3)} \\
 &= \frac{1}{6}(1212.65 \text{ MeV}/c^2) + \frac{1}{6}(1118.918 \text{ MeV}/c^2) \\
 &\quad + \frac{2}{3}(1116.725 \text{ MeV}/c^2) \\
 &= 1133.073333 \text{ MeV}/c^2
 \end{aligned} \tag{5.19}$$

Instead, if the quark masses and A' are adjusted to fit the experimental values of m_{Σ^0} and m_{Λ^0} , setting

$$\begin{aligned}
 m_u + m_d + m_s + \frac{A'}{4} \left(\frac{1}{3m_u m_d} - \frac{2}{3m_u m_s} - \frac{2}{3m_d m_s} \right) &= 1192.65 \text{ MeV}/c^2 \\
 m_u + m_d + m_s + \frac{A'}{4} \left(-\frac{2}{m_u m_d} - \frac{2}{m_u m_s} + \frac{1}{m_d m_s} \right) &= 1115.83 \text{ MeV}/c^2,
 \end{aligned} \tag{5.20}$$

gives

$$\frac{A'}{4} \left(\frac{1}{m_u m_d} - \frac{1}{m_d m_s} \right) = 76.82 \text{ MeV}/c^2 \tag{5.21}$$

Let $m_u = m_{ui} - \delta m$, $m_d = m_{di} - \delta m$ and $m_s = m_{si} - \delta m$, where m_{ui} , m_{di}

and m_{si} are the values of the masses listed after Eq.(5.4). Then

$$\begin{aligned}
 & \frac{A'}{4} \left[\left(\frac{1}{m_{ui}m_{di}} - \frac{1}{m_{di}m_{si}} \right) + \delta m \left(\frac{1}{m_{ui}^2 m_{di}} + \frac{1}{m_{ui} m_{di}^2} - \frac{1}{m_{di}^2 m_{si}} \right. \right. \\
 & \quad \left. \left. - \frac{1}{m_{di} m_{si}^2} \right) \right] + \mathcal{O} \left(\frac{\delta m^2}{m} \right) = 76.82 \text{ MeV}/c^2 \\
 & -3\delta m + \frac{A'}{4} \left[\left(\frac{1}{3m_{ui}m_{di}} - \frac{2}{3m_{ui}m_{si}} - \frac{2}{3m_{di}m_{si}} \right) + \delta m \left(\frac{1}{3m_{ui}^2 m_{di}} \right. \right. \\
 & \quad \left. \left. + \frac{1}{3m_{ui} m_{di}^2} - \frac{2}{3m_{ui}^2 m_{si}} - \frac{2}{3m_{ui} m_{si}^2} - \frac{2}{3m_{di}^2 m_{si}} - \frac{2}{3m_{di} m_{si}^2} \right) \right] \\
 & \quad + \mathcal{O} \left(\frac{\delta m^2}{m} \right) = -72.082 \text{ MeV}/c^2
 \end{aligned} \tag{5.22}$$

Substituting the values of m_{ui} , m_{di} and m_{si} into Eq.(5.22),

$$\begin{aligned}
 & \frac{A'}{4} \left[2.459655981(\text{GeV}/c^2)^{-2} + \delta m(18.09535536(\text{GeV}/c^2)^{-3}) \right] \\
 & \quad = 0.07682 \text{ GeV}/c^2 \\
 & -3\delta m + \frac{A'}{4} \left[-4.30556606(\text{GeV}/c^2)^{-2} - \delta m(17.620320156(\text{GeV}/c^2)^{-3}) \right] \\
 & \quad = -0.072082 \text{ GeV}/c^2
 \end{aligned} \tag{5.23}$$

Then

$$A' = \frac{0.30728 \text{ GeV}/c^2}{\left[2.4596554481 (\text{GeV}/c^2)^{-2} + \delta m(18.09533536 (\text{GeV}/c^2)^{-3}) \right]}. \tag{5.24}$$

and

$$\begin{aligned}
 & 54.2860668(\delta m)^2 + (8.73255933868 \text{ GeV}/c^2)\delta m \\
 & \quad + 0.153456700719 (\text{GeV}/c^2)^2 = 0.
 \end{aligned} \tag{5.25}$$

which has the roots

$$\delta m = \begin{cases} -0.020078190371 \text{ GeV}/c^2 \\ -0.14083705599 \text{ GeV}/c^2 \end{cases} \quad (5.26)$$

The upper root, equal to $-20.078190371 \text{ MeV}/c^2$, is the only phenomenologically realistic choice. The quark masses matching the experimentally measured masses of Σ^0 and Λ^0 with a weighting of up and down spins in the $\frac{1}{2}^+$ quantum state would be

$$\begin{aligned} m_{um}^{weighted} &= 382.078190371 \text{ MeV}/c^2 \\ m_{dm}^{weighted} &= 386.078190371 \text{ MeV}/c^2 \\ m_{sm}^{weighted} &= 557.078190371 \text{ MeV}/c^2. \end{aligned} \quad (5.27)$$

By Eq.(5.24),

$$A'_m{}^{weighted} = 0.14659705588 (\text{GeV}/c^2)^3. \quad (5.28)$$

These values in the weighted quantum state are considerably larger than the quark masses and coefficient in the literature. Therefore, it is likely that the initial set $m_{ui} = 362 \text{ MeV}/c^2$, $m_{di} = 366 \text{ MeV}/c^2$, $m_{si} = 537 \text{ GeV}/c^2$ and $A' = 0.078 (\text{GeV}/c^2)^3$ would be better for phenomenological calculations.

Nevertheless, it is necessary in general to define a symmetric two-quark state before constructing the three-quark wavefunction. The difference between Σ^0 and Λ^0 may be attributable, to some degree, to the groupings of the quarks.

References

- [1] R. D. Schafer, An Introduction to Nonassociative Algebras, Academic Press, New York, 1966.

- [2] Th. Motzkin, Relations between Hypersurface Cross Ratios, and a Combinatorial Formula for Partitions of a Polygon, for Permanent Preponderance, and for Nonassociative Products, Bull. Amer. Math. Soc. **54** (1948) 352-360.

- [3] M. Bremner and I. Hentzel, Invariant Nonassociative Algebra Structures on Irreducible Representations of Simple Lie Algebras, Exp. Math. **13** (2004) 231-256.

- [4] C. Patrignani et. al. (Particle Data Group), Chin. Phys. C **40** (2016) 100001.

FRUTE LOOPS *†

Tèmitópé Gbólàhàn Jaiyéolá ‡

Adesola Adefemi Adeniregun

Department of Mathematics, Obafemi Awolowo University
Ile Ife 220005, Nigeria

tjayeola@oauife.edu.ng, dessygirl247@yahoo.com

Oyeyemi Oluwaseyi Oyebola

Faculty of Education, Brandon University
Brandon Manitoba, Canada

oooyeyemi@gmail.com, oyeboloo65@brandonu.ca

Adedayo Oke Adelakun

Department of Physics, Federal University of Technology
Akure, Ondo State, Nigeria

aoadelakun@futa.edu.ng, d_onescientist@yahoo.com

Received July 16, 2021

Revised July 18, 2021

Abstract

A loop $(Q, \cdot)$ is called a FRUTE loop if it obeys the identity $(x \cdot xy)z = (y \cdot zx)x$. Interestingly, a FRUTE loop is a Moufang loop, but not necessarily an extra loop or a group (and vice versa). In this paper, some new algebraic properties of a FRUTE loop are established. It is shown that a FRUTE loop is centrum square, a middle A-loop and obeys the law $x^{-1}yx = xyx^{-1}$. It is proved that in a FRUTE loop, the following loops are equivalent: central square loop, group, extra loop, LC-loop, RC-loop, C-loop, LNS-loop, RNS-loop, MNS-loop, left Cheban loop, right Cheban loop, Cheban loop, LCC-loop, RCC-loop and CC-loop.

*2020 Mathematics Subject Classification. Primary 20N02, 20N05

†**Keywords and Phrases** : Moufang loop, FRUTE loop, group

‡All correspondence to be addressed to this author.

1 Introduction

Let G be a non-empty set. Define a binary operation $(\cdot)$ on G . If $x \cdot y \in G$ for all $x, y \in G$, then the pair $(G, \cdot)$ is called a *groupoid* or *magma*.

If each of the equations:

$$a \cdot x = b \quad \text{and} \quad y \cdot a = b$$

has unique solutions in G for x and y respectively, then $(G, \cdot)$ is called a *quasigroup*.

If there exists a unique element $e \in G$ called the *identity element* such that for all $x \in G$, $x \cdot e = e \cdot x = x$, $(G, \cdot)$ is called a *loop*. We write xy instead of $x \cdot y$, and stipulate that $\cdot$ has lower priority than juxtaposition among factors to be multiplied. For instance, $x \cdot yz$ stands for $x(yz)$.

Let x be a fixed element in a groupoid $(G, \cdot)$. The left and right translation maps of G , L_x and R_x respectively can be defined by

$$yL_x = x \cdot y \quad \text{and} \quad yR_x = y \cdot x.$$

It can now be seen that a groupoid $(G, \cdot)$ is a quasigroup if its left and right translation mappings are permutations. Since the left and right translation mappings of a quasigroup are bijective, then the inverse mappings L_x^{-1} and R_x^{-1} exist. Let

$$x \backslash y = yL_x^{-1} \quad \text{and} \quad x / y = xR_y^{-1}$$

and note that

$$x \backslash y = z \Leftrightarrow x \cdot z = y \quad \text{and} \quad x / y = z \Leftrightarrow z \cdot y = x.$$

In a loop $(G, \cdot)$ with identity element e , the *left inverse element* of $x \in G$ is the element $xJ_\lambda = x^\lambda \in G$ such that

$$x^\lambda \cdot x = e$$

while the *right inverse element* of $x \in G$ is the element $xJ_\rho = x^\rho \in G$ such that

$$x \cdot x^\rho = e.$$

For an overview of the theory of loops, readers may check [2, 3, 5, 8, 10, 20, 26, 27].

Below are the definitions of some basic loop properties which are at times naturally found to be true in a loop $(L, \cdot)$ of Bol-Moufang type.

A loop $(L, \cdot)$ is called a right inverse property loop (RIPL) if it satisfies right inverse property (RIP)

$$(yx)x^\rho = y \quad (1)$$

A loop $(L, \cdot)$ is called a left inverse property loop (LIPL) if it satisfies left inverse property (LIP)

$$x^\lambda(xy) = y \quad (2)$$

A loop $(L, \cdot)$ is called an inverse property loop (IPL) if it is both a LIPL and RIPL.

A loop $(L, \cdot)$ is called a cross inverse property loop (CIPL) if it satisfies cross inverse property (CIP)

$$x(yx^\rho) = y \quad \text{or} \quad x^\lambda(yx) = y \quad (3)$$

A loop $(L, \cdot, \backslash, /)$ is called a left conjugacy closed loop (LCCL) if it satisfies the equation $z \cdot yx = ((zy)/z) \cdot zx$ and a right conjugacy closed loop (RCCL) if it satisfies the equation $xy \cdot z = xz \cdot (z \backslash (yz))$. A loop $(L, \cdot, \backslash, /)$ is called a conjugacy closed loop (CCL) if it is both an LCCL and a RCCL. A loop $(L, \cdot, \backslash, /)$ is called a van Rees loop if it obeys the identities $x(y \backslash (xz)) = y(x \backslash (yz))$ and $((xy)/z)y = ((xz)/y)z$.

Let a, b and c be three elements of a loop L . The loop associator of a, b and c is the unique element (a, b, c) of L which satisfies $(ab)c = \{a(bc)\}(a, b, c)$.

The right nucleus of L is defined by $N_\rho(L, \cdot) = \{x \in L \mid zy \cdot x = z \cdot yx \ \forall y, z \in L\}$. The left nucleus of L is defined by $N_\lambda(L, \cdot) = \{a \in L : ax \cdot y = a \cdot xy \ \forall x, y \in L\}$. The middle nucleus of L is defined by $N_\mu(L, \cdot) = \{a \in L : ya \cdot x = y \cdot ax \ \forall x, y \in L\}$. The nucleus of L is defined by $N(L, \cdot) = N_\lambda(L, \cdot) \cap N_\rho(L, \cdot) \cap N_\mu(L, \cdot)$. The centrum of L is defined by $C(L, \cdot) = \{a \in L : ax = xa \ \forall x \in L\}$. The center of L is defined by $Z(L, \cdot) = N(L, \cdot) \cap C(L, \cdot)$. $N_\rho(L, \cdot), N_\lambda(L, \cdot), N_\mu(L, \cdot), N(L, \cdot), Z(L, \cdot)$ are subgroups of $(L, \cdot)$.

The triple (A, B, C) of bijections of a loop $(G, \cdot)$ is called an autotopism if

$$xA \cdot yB = (x \cdot y)C \ \forall x, y \in G. \quad (4)$$

Such triples form a group $AUT(G, \cdot)$ called the autotopism group of $(G, \cdot)$. Furthermore, if $A = B = C$, then A is called an automorphism of $(G, \cdot)$.

Such bijections form a group $AUM(G, \cdot)$ called the automorphism group of $(G, \cdot)$.

The group of all permutations on G is called the permutation group of G and denoted by $SYM(G)$. The group $\mathcal{M}(G, \cdot) = \langle \{R_x, R_x^{-1}, L_x, L_x^{-1} : x \in G\} \rangle$ is called the multiplication group of $(G, \cdot)$ and $\mathcal{M}(G, \cdot) \leq SYM(G)$. An element $\alpha \in \mathcal{M}(G, \cdot)$ such that $e\alpha = e$ is called an inner mapping of $(G, \cdot)$. The inner mapping $T(x) = R_x L_x^{-1}$ is called a middle inner mapping and the group generated by all such is called the middle inner mapping group $\text{Inn}_\mu(G, \cdot) = \langle T(x) \mid x, y \in G \rangle$. A loop $(G, \cdot)$ in which $\text{Inn}_\mu(G, \cdot) \leq AUM(G, \cdot)$ is called a middle A-loop (A_μ -loop).

1.1 Identities of Bol-Moufang Type

Among all the 60 identities (30 of which are equivalent to associativity in loops) called identities of Bol-Moufang type (these are variety of loops defined by a single identity that : (i) involves three distinct variables on both sides, (ii) contains variables in the same order on both sides, (iii) exactly one of the variables appears twice on both sides) which characterize loops is found a type of loop that satisfies what is called the 'right-Bol identity' ('left-Bol identity') as named by Ferenc Fenyves [6] and [7] in 1968 and 1969 respectively. Loops that satisfy the right (left) Bol identity are called 'right (left) Bol loops'. Closely related to the 'right-Bol identity' ('left-Bol identity') are the extra and Moufang identities. Some other loops of Bol-Moufang type which seem to deviate (see the hasse diagram on page 8) from the Bol, extra and Moufang loops are the left central (LC-), right central (RC-), central (C-), left nuclear square (LNS-), right nuclear square (RNS-) and middle nuclear square (MNS-) loops. The formulas which some of these identities obey are stated below as found in [7].

$$(yx \cdot x)z = y(x \cdot xz) \text{ central identity} \quad (5)$$

$$(xy \cdot z)x = x(y \cdot zx) \text{ extra identity} \quad (6)$$

$$xy \cdot xz = x(yx \cdot z) \text{ extra identity} \quad (7)$$

$$yx \cdot zx = (y \cdot xz)x \text{ extra identity} \quad (8)$$

$$xx \cdot yz = (x \cdot xy)z \text{ left central identity} \quad (9)$$

$$(x \cdot xy)z = x(x \cdot yz) \text{ left central identity} \quad (10)$$

$$(xx \cdot y)z = x(x \cdot yz) \quad \text{left central identity} \quad (11)$$

$$(y \cdot xx)z = y(x \cdot xz) \quad \text{left central identity} \quad (12)$$

$$yz \cdot xx = y(zx \cdot x) \quad \text{right central identity} \quad (13)$$

$$(yz \cdot x)x = y(zx \cdot x) \quad \text{right central identity} \quad (14)$$

$$(yz \cdot x)x = y(z \cdot xx) \quad \text{right central identity} \quad (15)$$

$$(yx \cdot x)z = y(xx \cdot z) \quad \text{right central identity} \quad (16)$$

$$(xx)(yz) = ((xx)y)z \quad \text{left nuclear square identity} \quad (17)$$

$$x(y(zz)) = (xy)(zz) \quad \text{right nuclear square identity} \quad (18)$$

$$x((yy)z) = (x(yy))z \quad \text{middle nuclear square identity} \quad (19)$$

$$xy \cdot zx = (x \cdot yz)x \quad \text{Moufang identity} \quad (20)$$

$$xy \cdot zx = x(yz \cdot x) \quad \text{Moufang identity} \quad (21)$$

$$(xy \cdot x)z = x(y \cdot xz) \quad \text{Moufang identity} \quad (22)$$

$$(yx \cdot z)x = y(x \cdot zx) \quad \text{Moufang identity} \quad (23)$$

$$(x \cdot yx)z = x(y \cdot xz) \quad \text{left Bol identity} \quad (24)$$

$$(yx \cdot z)x = y(xz \cdot x) \quad \text{right Bol identity} \quad (25)$$

In any loop, there is equivalence between any two of the identities corresponding to each of the equation numbers in each of the triples $\{(6), (7), (8)\}$, $\{(9), (10), (11), (12)\}$ and $\{(13), (14), (15), (16)\}$. These facts are found in [6], [7] and [23]. In fact, in a loop, any one of (9), (10), (11), (12) and any one of (13), (14), (15), (16) together is equivalent to (5) and vice versa. Although in a loop, any one of (6), (7), (8) implies (5), the converse is not true. Loops that satisfy (9) and (13) or their equivalent forms are called left central and right central loops, in short LC-loops and RC-loops respectively. Their algebraic properties can be found in Adéníran and Jaiyéólá [1], Jaiyéólá and Adéníran [13, 14, 15, 16] and Jaiyéólá [11, 12].

1.2 Identities of Generalized Bol-Moufang Type

In 2011, Cote et al. [4] embarked upon the classification of generalized Bol-Moufang type, a generalization of the classification of loops of Bol-Moufang type which was originally initiated by Ferenc Fenyves [6] and [7] in 1968 and 1969 respectively and completed by Phillips and Vojtěchovský [23] in 2005. By generalized Bol-Moufang type, we mean those identities in which the variables do not appear in the same order of both sides in the identity. The following scheme in Table 1 was used to label each identity. This is a reformulation of the labeling scheme used by Phillips and Vojtěchovský [23].

Variable Order				Multiplication Order	
A	xyz	G	xzy	1	$a(b(cd))$
B	$xyxz$	H	$xzxy$	2	$a((bc)c)$
C	$yxxz$	I	zxy	3	$(ab)(cd)$
D	$xyzx$	J	$xzyx$	4	$(a(bc))d$
E	$yxzx$	K	$zxyx$	5	$((ab)c)d$
F	$yzxx$	L	$zyxx$		

Table 1: Scheme for Labelling Identities of Generalized Bol-Moufang Type

For example, the identity $(x(xy))z = (y(zx))x$ is called A4F4. In order to classify all varieties of loops of generalized Bol-Moufang type, Cote et al. [4] first counted all possible identities of generalized Bol-Moufang type, 1215 in all. They then found equivalences among these identities, systematically examining and eliminating first equivalent commutative identities (1092) and then equivalent non-commutative identities. It was observed that any commutative identity of the generalized Bol-Moufang type can either be commuted to be of the Bol-Moufang or is of the commutative Moufang variety. The remainder is the list of unique varieties, which they called loops of Perfect type. For those identities in which the variables do not appear in the same order on both sides, it was shown that the identities are 48 varieties:

1. the 14 varieties of Bol-Moufang type (Phillips and Vojtěchovský [23]),
2. the 6 varieties of commutative Bol-Moufang type,
3. and 28 new varieties.

Since 28 is a perfect number, the authors called the new varieties Perfect Varieties. The authors were aided in their research with the use of Prover9, an automated theorem prover, and Mace4, a finite model builder. A few of the 28 Perfect identities which are relevant to this present study are listed in Table 2

Variety	Abbreviation	Defining Identity	Its Name
Cheban 1 (Left Cheban)	C1	$x((xy)z) = (yx)(xz)$	A2C3
Cheban 2 (Cheban)	C2	$x((xy)z) = (y(zx))x$	A2F4
Cheban I Dual (Right Cheban)	CD	$(yx)(xz) = (y(zx))x$	C3F4
Frute	FR	$(x(xy))z = (y(zx))x$	A4F4
Crazy Loop	CR	$(x(xy))z = (yx)(xz)$	A4C3

Table 2: Few Varieties of Perfect Identities

New varieties in Table 2 are primarily named according to the number of Perfect identities that axiomatize them. The *FRUTE* variety is an acronym of the structural properties of A4F4 which is of key interest in this study. A4C3 is named because it implies all of the Bol-Moufang varieties, which some may consider crazy. Like we mentioned above, this current study is based on FRUTE loops. They are described by 12 equivalent identities, namely: A4F4, A2C1, A2C2, A3C3, A1C3, A2F1, A2F2, A5F4, C3F3, C3F5, C4F4 and C5F4.

1.3 Existing Results on Frute loops

According to the 2011 work of Cote et al. [4] on the classification of loops of generalized Bol-Moufang type, the identity A4F4 which defines FRUTE loops contains the most interesting structural properties of any variety of Perfect type. They called A4F4 the *FRUTE* variety because A4F4 is Flexible, Right bol and left bol, Unity of R.Alt and L.Alt, Three-power associative and Entails both Osborn and Moufang properties.

Jaiyéolá et al. [17] observed that the Quaternion group Q_8 is one of the smallest non-commutative FRUTE loops of order 8, there are 2 non-associative commutative FRUTE loops of order 81 up to isomorphism and there exists a non-associative and non-commutative FRUTE loop of order 648. In 2019, Phillips [21] mentioned that apart from FRUTE loops, Moufang loops, commutative Moufang loops, extra loops, there are no other generalized Bol-Moufang loop varieties of non-associative, Moufang loops. Hence, FRUTE loops are the final Moufang frontier.

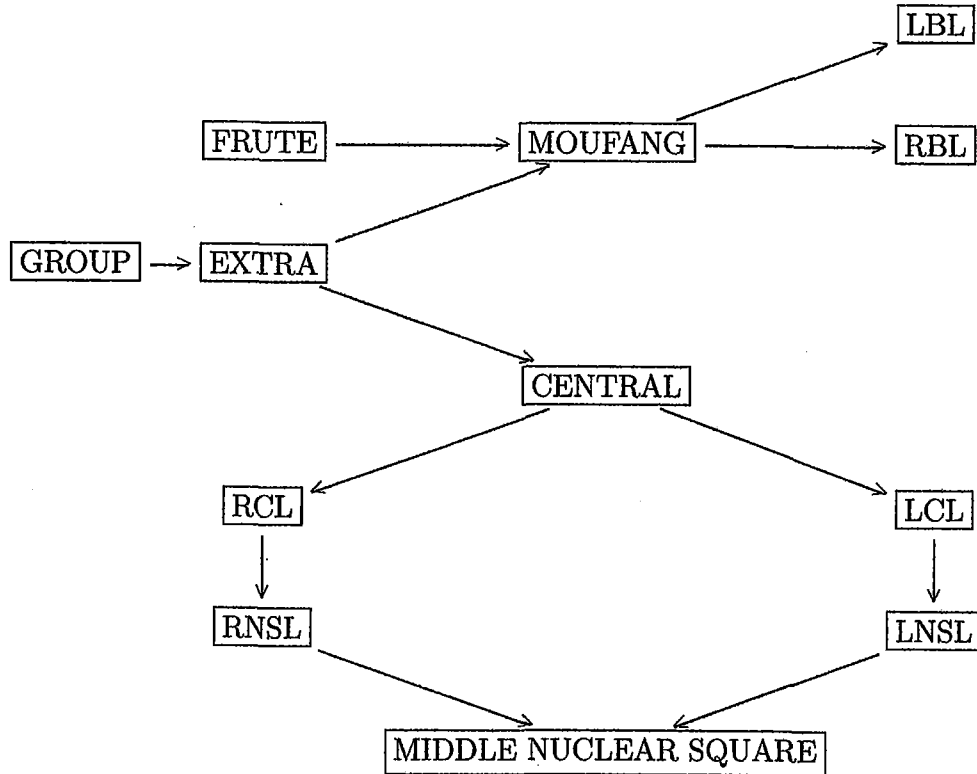
Here are some relevant results on generalized Bol-Moufang type of loops:

Theorem 1.1. (Cote et al.[4], 2011)

The following identities are equivalent in a loop: A_4F_4 , A_2C_1 , A_2C_2 , A_3C_3 , A_1C_3 , A_2F_1 , A_2F_2 , A_5F_4 , C_3F_3 , C_3F_5 , C_4F_4 and C_5F_4 .

Theorem 1.2. (Cote et al.[4], 2011)

A FRUTE loop is a Moufang loop.



The objectives of this research are as follows:

- to establish new algebraic properties of FRUTE loops;
- to establish necessary or (and) sufficient condition(s) for a right-Bol loop, left-Bol loop, Moufang loop, left central loop, right central loop, central loop, left Cheban loop, right Cheban loop, Cheban loop, LCC-loop, RCC-loop, CC-loop, extra loop and a group to be a FRUTE loop.

In this paper, some new algebraic properties of a FRUTE loop are established. It is shown that a FRUTE loop is centrum square, a middle A-loop and obeys the law $x^{-1}yx = xyx^{-1}$. In a FRUTE loop $(Q, \cdot)$, the following are true: $x^{2k} \in C(Q, \cdot)$, $x^{3k} \in N(Q, \cdot)$, $x^{6k} \in Z(Q, \cdot)$, $\langle x^3 \rangle \leq N(Q, \cdot)$, $\langle x^6 \rangle \leq Z(Q, \cdot)$ for all $x \in Q$, $k \in \mathbb{Z}$ where $C(Q, \cdot)$, $N(Q, \cdot)$ and $Z(Q, \cdot)$ are respectively the centrum, nucleus and center of $(Q, \cdot)$. Any commutative right (left) Bol loop or Moufang loop is shown to be a FRUTE loop while a group is shown to be a FRUTE loop if and only if it is a central square loop. A FRUTE loop is shown to be a cross inverse property loop if and only if it is a commutative loop if and only if it is central cube if and only if it obeys the identity $(xy)^2 = x^2y^2$. A FRUTE loop is shown to be of exponent 2 if and only if it obeys the identity $(xyx)(xzx) = x(yz)x$. Some sufficient condition(s) for right (left) Bol loop and Moufang loop to be a FRUTE loop and a van Rees loop are established. Associativity is established as a necessary and sufficient condition for which particular types of the following loops to be FRUTE loops: LC-loop, RC-loop, C-loop, LNS-loop, RNS-loop and MNS-loop. It is proved that in a FRUTE loop, the following loops are equivalent: central square loop, group, extra loop, LC-loop, RC-loop, C-loop, LNS-loop, RNS-loop, MNS-loop, left Cheban loop, right Cheban loop, Cheban loop, LCC-loop, RCC-loop and CC-loop.

We shall need the following results to achieve our objectives.

Lemma 1.1. *Let $(G, \cdot)$ be a loop.*

1. *Then the following are equivalent for all $x \in G$:*

- (a) $(G, \cdot)$ is a Moufang loop.
- (b) $M_1 = (L_x, R_x, L_x R_x) \in \text{AUT}(G, \cdot)$.
- (c) $M_2 = (L_x, R_x, R_x L_x) \in \text{AUT}(G, \cdot)$.

- (d) $M_3 = (L_x R_x, L_x^{-1}, L_x) \in \text{AUT}(G, \cdot)$.
- (e) $M_4 = (R_y^{-1}, R_y L_y, R_y) \in \text{AUT}(G, \cdot)$.
- 2. $(G, \cdot)$ is a Right-Bol loop $RB = (R_y^{-1}, L_y R_y, R_y) \in \text{AUT}(G, \cdot)$.
- 3. $(G, \cdot)$ is a Left-Bol loop $LB = (R_x L_x, L_x^{-1}, L_x) \in \text{AUT}(G, \cdot)$.

Theorem 1.3. (Fenyves [7])

Let $(G, \cdot)$ be a loop. The following statements are equivalent:

- 1. $(G, \cdot)$ is an extra loop,
- 2. $(G, \cdot)$ is a Moufang loop and x^2 lies in the nucleus of $(G, \cdot)$ for every $x \in G$.

Theorem 1.4. (Phillips and Shcherbacov [22])

- 1. A loop Q is a left (right) Cheban loop if and only if it is an LCCL (RCCL) and $R_x^2 = L_x^2$ for all $x \in Q$.
- 2. A loop is a Cheban loop if and only if it is both a left and a right Cheban loop.
- 3. Let Q be a left Cheban loop. If Q is a WIPL or if $R_{x^2} = L_{x^2}$ for all $x \in Q$, then Q is a Cheban loop.
- 4. Let Q be a left Cheban loop. If Q is flexible or a RAPL, then Q is an extra loop and a Cheban loop.
- 5. In a cancellative CC-groupoid Q , the following two conditions are equivalent:
 - (a) $R_{x^2} = L_{x^2}$ for all $x \in Q$.
 - (b) $R_x^2 = L_x^2$ for all $x \in Q$.
- 6. A loop Q is a Cheban loop if and only if Q is a CCL and satisfies $R_{x^2} = L_{x^2}$ for all $x \in Q$.
- 7. A Cheban loop is a WIP power associative CCL.

Theorem 1.5. (Kinyon and Wanless [19])

A left (right) Bol loop of exponent 3 is a van Rees loop.

2 Main Results

Theorem 2.1. *Let $(G, \cdot)$ be a loop.*

1. *A centrum square LC-loop $(G, \cdot)$ is a Frute loop if and only if $(G, \cdot)$ is a group.*
2. *An LNSL $(G, \cdot)$ with $x^2 \in C(G, \cdot)$ and RAP is a Frute loop if and only if $(G, \cdot)$ is a group.*
3. *For a MNSL $(G, \cdot)$ with $x^2 \in C(G, \cdot)$ and RAP (LAP), $(G, \cdot)$ is a Frute loop if and only if $(G, \cdot)$ is a group.*
4. *For a C-loop $(G, \cdot)$ with $x^2 \in C(G, \cdot)$, $(G, \cdot)$ is a Frute loop if and only if $(G, \cdot)$ is a group.*
5. *For a RNSL $(G, \cdot)$ with $x^2 \in C(G, \cdot)$ and LAP, $(G, \cdot)$ is a Frute loop if and only if $(G, \cdot)$ is a group.*
6. *For a RC-loop $(G, \cdot)$ with $x^2 \in C(G, \cdot)$ and RAP, $(G, \cdot)$ is a Frute loop if and only if $(G, \cdot)$ is a group.*
7. *Every group of exponent 2 is a Frute loop.*
8. *An abelian group is a Frute loop.*
9. *A central square group is a Frute loop.*

Proof. 1. We target a necessary and sufficient condition for A2C1: $x(xy \cdot z) = y(x \cdot xz)$ to hold. If $(G, \cdot)$ is a centrum square LC-loop, then $\text{R.H.S(A2C1)} = y(x \cdot xz) \stackrel{(12)}{=} (y \cdot xx)z \stackrel{x^2 \in C(G, \cdot)}{=} x^2 y \cdot z \stackrel{\text{LAP}}{=} (x \cdot xy)z$. Note that $x(xy \cdot z) = (x \cdot xy)z \cdot (x, xy, z)$ in any loop. And so, if $(G, \cdot)$ is a group, then $(x, xy, z) = e \Rightarrow \text{R.H.S(A2C1)} = (x \cdot xy)z = x(xy \cdot z) = \text{L.H.S(A2C1)} \Rightarrow (G, \cdot)$ is a Frute loop. Conversely, if $(G, \cdot)$ is a Frute loop, then $(x, xy, z) = e \xrightarrow[\text{IP}]{y \mapsto x^{-1}y} (x, y, z) = e \Rightarrow (G, \cdot)$ is a group.

2. We target a necessary and sufficient condition for A3C3: $(xx)(yz) = (yx)(xz)$ to hold. $\text{L.H.S} = (xx)(yz) \stackrel{(17)}{=} (xx \cdot y)z \stackrel{x^2 \in C(G, \cdot)}{=} (y \cdot xx)z \stackrel{\text{RAP}}{=} (yx \cdot x)z$. Now, $(yx \cdot x)z = (yx \cdot xz)(yx, x, z)$, so the rest and the converse follow similarly as in 1.

3. We target a necessary and sufficient condition for C4F4: $(y \cdot xx)z = (y \cdot zx)x$ to hold. L.H.S $= (y \cdot xx)z \stackrel{(19)}{=} y(xx \cdot z) \stackrel{x^2 \in C(G, \cdot)}{=} y(z \cdot xx) \stackrel{\text{RAP}}{=} y(zx \cdot x)$. Now, $y(zx \cdot x) = (y \cdot zx)x \cdot (y, zx, x)$, so the rest and the converse follow similarly as in 1. The second part (for the LAP case) is gotten by targetting the identity A2C2 for FRUTE loops, which is the dual of C4F4.
- 4, 7, 8 and 9 follow from 1, 5 is the dual of 2 and 6 is the dual of 1. $\square$

Theorem 2.2. 1. A Frute loop is a centrum square.

2. A Frute loop is a CIPL if and only if it is commutative.
3. (a) A Frute loop is a group if and only if it is central square.
(b) A group is a Frute loop if and only if it is central square.
4. A Frute loop is group if and only if it is an extra loop.
5. A Frute loop is an LC-loop if and only if it is an RC-loop if and only if it is a group if and only if it is an LNSL if and only if it is an RNSL if and only if it is an MNSL if and only if it is a C-loop.

Proof. 1. Consider A4F4: $(x \cdot xy)z = (y \cdot zx)x$. Note that Frute loop has RAP since it is Moufang (Theorem 1.2). Now, put $y = e$, then $(x \cdot xe)z = (e \cdot zx)x \Rightarrow (x \cdot x)z = (zx)x \Rightarrow x^2z = zx^2 \Rightarrow x^2 \in C(G, \cdot)$.

2. Consider A4F4: $(x \cdot xy)z = (y \cdot zx)x$. Put $y = x^\rho = x^\lambda = x^{-1}$ (since a Frute loop is a Moufang loop, its elements have two-sided inverses), then $(x \cdot xx^{-1})z = (x^{-1} \cdot zx)x \Rightarrow xz = (x^{-1} \cdot zx)x \Rightarrow xz = zx$.

Conversely, a Frute loop has the LIP, hence with commutativity,

$$x^{-1}(yx) = x^{-1}(xy) = y \Rightarrow x^{-1}(yx) = y, \text{ the CIP.}$$

3. (a) Let L be a Frute loop that is a group, then L is central square. Conversely, let L be a Frute loop, then, $(x \cdot xy)z = (y \cdot zx)x \Rightarrow (x^2y)z = (y \cdot zx)x$. If $x^2 \in Z(L)$, then $(yx^2)z = (y \cdot zx)x \stackrel{\text{C3F5}}{\stackrel{\text{C3F3}}{=}} (yz \cdot x)x = (y \cdot zx)x \Rightarrow yz \cdot x = y \cdot zx$.
- (b) $x(xy \cdot z) = y(x \cdot xz) \Leftrightarrow x^2yz = yx^2z \Leftrightarrow x^2y \cdot z = yx^2 \cdot z \Leftrightarrow x^2y = yx^2$.
4. This follows from Theorem 1.3 and 3, based on the fact that a Frute loop is a Moufang loop.

5. Since a Frute loop has the hypotheses in this case, use 1 to 3 of Theorem 2.1.

□

Corollary 2.1. *Let $(G, \cdot)$ be a Frute loop. Then the following are equivalent:*

- | | |
|---|--|
| 1. $(G, \cdot)$ is a central square loop. | 7. $(G, \cdot)$ is a middle nuclear square loop. |
| 2. $(G, \cdot)$ is a group. | |
| 3. $(G, \cdot)$ is an extra loop. | 8. $(G, \cdot)$ is a left nuclear square loop. |
| 4. $(G, \cdot)$ is an RC-loop. | |
| 5. $(G, \cdot)$ is an LC-loop. | 9. $(G, \cdot)$ is a right nuclear square loop. |
| 6. $(G, \cdot)$ is a central loop. | |

Proof. This follows from Theorem 2.2.

□

Theorem 2.3. *Let G be a Frute loop. Then the following are equivalent:*

- | | |
|--------------------------------|------------------------|
| 1. G is a group. | 5. G is an LCC-loop. |
| 2. G is a Cheban loop. | |
| 3. G is a left Cheban loop. | 6. G is an RCC-loop. |
| 4. G is a right Cheban loop. | 7. G is a CC-loop. |

Proof. We shall employ Theorem 1.4 appropriately.

1. $\Leftrightarrow$ 3. G is a Frute loop $\xLeftrightarrow{A2C1} L_{xy}L_x = L_x^2L_y \Leftrightarrow L_x^2L_y = L_{xy}L_x \Leftrightarrow L_x^2L_yL_{yx}^{-1} = L_{xy}L_xL_{yx}^{-1} \Leftrightarrow L_xL_xL_yL_{yx}^{-1} = L_{xy}L_xL_{yx}^{-1} \Leftrightarrow L_x^{-1}L_xL_xL_yL_{yx}^{-1} = L_x^{-1}L_{xy}L_xL_{yx} \Leftrightarrow L_xL_yL_{yx}^{-1} = L_x^{-1}L_{xy}L_xL_{yx}^{-1} \Leftrightarrow L_{(x,y)} = L_x^{-1}L_{xy}L_xL_{yx}^{-1}$. A Frute loop G is associative $\Leftrightarrow L_{(x,y)} = I \Leftrightarrow L_x^{-1}L_{xy}L_xL_{yx}^{-1} = I \Leftrightarrow L_{xy}L_x = L_xL_{yx} \Leftrightarrow zL_{xy}L_x = zL_xL_{yx} \Leftrightarrow x(xy \cdot z) = (yx)(xz) \Leftrightarrow G$ is a left Cheban loop.
1. $\Leftrightarrow$ 2. G is a Frute loop $\xLeftrightarrow{A4F4} L_x^2R_z = R_{zx}R_x \Leftrightarrow L_x^{-1}L_xL_xR_z = L_x^{-1}R_{zx}R_x \Leftrightarrow L_xR_z = L_x^{-1}R_{zx}R_x \Leftrightarrow L_x^{-1}L_xR_z = L_x^{-1}L_x^{-1}R_{zx}R_x \Leftrightarrow R_z = L_x^{-1}L_x^{-1}R_{zx}R_x \Leftrightarrow R_zR_x = L_x^{-1}L_x^{-1}R_{zx}R_xR_x \Leftrightarrow R_zR_xR_{zx}^{-1} = L_x^{-1}L_x^{-1}R_{zx}R_xR_xR_{zx}^{-1} \Leftrightarrow R_{(z,x)} = L_x^{-1}L_x^{-1}R_{zx}R_xR_xR_{zx}^{-1}$.

A Frute loop G is associative $\Leftrightarrow R_{(z,x)} = I \Leftrightarrow L_x^{-1}L_x^{-1}R_{zx}R_xR_xR_{zx}^{-1} = I \Leftrightarrow R_{zx}R_xR_x = L_xL_xR_{zx} \Leftrightarrow yR_{zx}R_xR_x = yL_xL_xR_{zx} \Leftrightarrow ((y \cdot zx)x)x = (x \cdot xy)(zx) \stackrel{(20)}{\Leftrightarrow} ((y \cdot zx)x)x = (x(xy \cdot z))x \Leftrightarrow (y \cdot zx)x = x(xy \cdot z) \Leftrightarrow G$ is a Cheban loop.

- 1. $\Leftrightarrow$ 4. This is the dual of 1. $\Leftrightarrow$ 3.
- 1. $\Leftrightarrow$ 5. If G is a group, then it is a left Cheban, and then it is an LCCL by Theorem 1.4(1.). The converse is similar.
- 1. $\Leftrightarrow$ 6. This is the dual of 1. $\Leftrightarrow$ 5.
- 1. $\Leftrightarrow$ 7. Assume G is a group, then it is Cheban, and then it is a CCL by Theorem 1.4(6.). The converse is similar.

□

Lemma 2.1. *Let $(G, \cdot)$ be a loop. The following are equivalent for all $x \in G$:*

1. $(G, \cdot)$ is a Frute loop.
2. $F_1 = (L_x^2, R_x^{-1}, R_x) \in \text{AUT}(G, \cdot)$.
3. $F_2 = (L_x^{-1}, L_x^2, L_x) \in \text{AUT}(G, \cdot)$.
4. $F_3 = (L_x^{-1}, L_{x^2}, L_x) \in \text{AUT}(G, \cdot)$.
5. $F_4 = (R_x, L_x, L_{x^2}) \in \text{AUT}(G, \cdot)$.
6. $F_5 = (R_x, L_x, L_x^2) \in \text{AUT}(G, \cdot)$.
7. $F_6 = (L_x^{-1}, R_{x^2}, L_x) \in \text{AUT}(G, \cdot)$.
8. $F_7 = (L_x^{-1}, R_x^2, L_x) \in \text{AUT}(G, \cdot)$.
9. $F_8 = (L_{x^2}, R_x^{-1}, R_x) \in \text{AUT}(G, \cdot)$.
10. $F_9 = (R_x, L_x, R_{x^2}) \in \text{AUT}(G, \cdot)$.
11. $F_{10} = (R_x, L_x, R_x^2) \in \text{AUT}(G, \cdot)$.
12. $F_{11} = (R_{x^2}, R_x^{-1}, R_x) \in \text{AUT}(G, \cdot)$.
13. $F_{12} = (R_x^2, R_x^{-1}, R_x) \in \text{AUT}(G, \cdot)$.

- Proof.* 1. $A4F4$ holds $\Leftrightarrow (x \cdot xy)z = (y \cdot zx)x \Leftrightarrow yL_x^2 \cdot z = (y \cdot zR_x)R_x \Leftrightarrow F_1 = (L_x^2, R_x^{-1}, R_x) \in AUT(G, \cdot)$.
2. $A2C1$ holds $\Leftrightarrow x(xy \cdot z) = y(x \cdot xz) \Leftrightarrow (yL_x \cdot z)L_x = y \cdot zL_xL_x \Leftrightarrow F_2 = (L_x^{-1}, L_x^2, L_x) \in AUT(G, \cdot)$.
3. $A2C2$ holds $\Leftrightarrow x(xy \cdot z) = y(xx \cdot z) \Leftrightarrow (yL_x \cdot z)L_x = y \cdot zL_{xx} \Leftrightarrow F_3 = (L_x^{-1}, L_{x^2}, L_x) \in AUT(G, \cdot)$.
4. $A3C3$ holds $\Leftrightarrow xx \cdot yz = yx \cdot xz \Leftrightarrow (yz)L_{xx} = yR_x \cdot zL_x \Leftrightarrow F_4 = (R_x, L_x, L_{x^2}) \in AUT(G, \cdot)$.
5. $A1C3$ holds $\Leftrightarrow x(x \cdot yz) = yx \cdot xz \Leftrightarrow (yz)L_xL_x = yR_x \cdot zL_x \Leftrightarrow F_5 = (R_x, L_x, L_x^2) \in AUT(G, \cdot)$.
6. $A2F1$ holds $\Leftrightarrow x(xy \cdot z) = y(z \cdot xx) \Leftrightarrow (yL_x \cdot z)L_x = y \cdot zR_{xx} \Leftrightarrow F_6 = (L_x^{-1}, R_{x^2}, L_x) \in AUT(G, \cdot)$.
7. $A2F2$ holds $\Leftrightarrow x(xy \cdot z) = y(zx \cdot x) \Leftrightarrow (yL_x \cdot z)L_x = y(zR_xR_x) \Leftrightarrow F_7 = (L_x^{-1}, R_x^2, L_x) \in AUT(G, \cdot)$.
8. $A5F4$ holds $\Leftrightarrow (xx \cdot y)z = (y \cdot zx)x \Leftrightarrow yL_{x^2} \cdot z = (y \cdot zR_x)R_x \Leftrightarrow F_8 = (L_{x^2}, R_x^{-1}, R_x) \in AUT(G, \cdot)$.
9. $C3F3$ holds $\Leftrightarrow yx \cdot xz = yz \cdot xx \Leftrightarrow yR_x \cdot zL_x = (yz)R_{x^2} \Leftrightarrow F_9 = (R_x, L_x, R_{x^2}) \in AUT(G, \cdot)$.
10. $C3F5$ holds $\Leftrightarrow yx \cdot xz = (yz \cdot x)x \Leftrightarrow yR_x \cdot zL_x = (yz)R_xR_x \Leftrightarrow F_{10} = (R_x, L_x, R_x^2) \in AUT(G, \cdot)$.
11. $C4F4$ holds $\Leftrightarrow (y \cdot xx)z = (y \cdot zx)x \Leftrightarrow yR_{x^2} \cdot z = (y \cdot zR_x)R_x \Leftrightarrow F_{11} = (R_{x^2}, R_x^{-1}, R_x) \in AUT(G, \cdot)$.
12. $C5F4$ holds $\Leftrightarrow (yx \cdot x)z = (y \cdot zx)x \Leftrightarrow yR_x^2 \cdot z = (y \cdot zR_x)R_x \Leftrightarrow F_{12} = (R_x^2, R_x^{-1}, R_x) \in AUT(G, \cdot)$.

□

Theorem 2.4. *In a FRUTE loop $(G, \cdot)$, the following are true for every $k \in \mathbb{Z}$:*

1. $x^{2k} \in C(G, \cdot)$.
3. $x^{6k} \in Z(G, \cdot)$.
5. $\langle x^6 \rangle \leq Z(G, \cdot)$.
2. $x^{3k} \in N(G, \cdot)$.
4. $\langle x^3 \rangle \leq N(G, \cdot)$.

Proof. 1. Since $x^2 \in C(G, \cdot)$, then $(x^k)^2 = x^{2k} \in C(G, \cdot)$ for all $k \in \mathbb{Z}$.

2. In a Frute loop, $N(G, \cdot)$ is a subgroup of $(G, \cdot)$.

$F_1M_1 = (L_x^3, I, L_xR_x^2)(G, \cdot) \Leftrightarrow x^3y \cdot z = x(yz)x^2 \Leftrightarrow x^3y \cdot z = x^3(yz) \Leftrightarrow x^3 \in N(G, \cdot)$. Thus, $(x^3)^k = x^{3k} \in N(G, \cdot)$ for all $k \in \mathbb{Z}$.

3. This follows from the fact that: $Z(G, \cdot) = N(G, \cdot) \cap C(G, \cdot)$.

4. By 2.

5. By 3.

□

Remark 2.1. In a power associative conjugacy closed loop Q , Kinyon and Kunen [18] proved that for every element $x \in Q$, x^3 is a the weak inverse element, x^6 is an extra element and $x^{12} \in N(Q)$. Whereas by Theorem 2.4, $x^3 \in N(Q)$, $x^6, x^{12} \in Z(Q)$ for a Frute loop Q . In an extra loop Q , $x^2 \in N(Q)$ but in a Frute loop Q , $x^2 \in C(Q)$.

Theorem 2.5. 1. In a right (left) Bol loop $(G, \cdot)$, if $x(xy) \cdot x = y = xy \cdot x^2$ ($x(yx \cdot x) = y = x^2 \cdot yx$), then $(G, \cdot)$ is a Frute loop and a van Rees loop.

2. In a right (left) Bol loop $(G, \cdot)$, if $(G, \cdot)$ is of exponent 3 and with centrum square property, then $(G, \cdot)$ is a Frute loop and a van Rees loop.

3. If $(G, \cdot)$ is a Moufang loop of exponent 3 with centrum square property, then $(G, \cdot)$ is a Frute loop and a van Rees loop.

4. A commutative Moufang loop is a Frute loop.

5. A commutative right (left) Bol loop is a Frute loop.

6. If $(G, \cdot)$ is a Moufang loop in which $x(yx)x = y$, then $(G, \cdot)$ is a Frute loop and a van Rees loop.

7. If $(G, \cdot)$ is a commutative extra loop, then $(G, \cdot)$ is a Frute loop.

Proof. We shall make use of Lemma 1.1 and Lemma 2.1.

1. $F_1 = RB$ if $R_x^{-1} = L_x^2$ and $L_x R_x = R_x^{-1}$.
 - (a) $R_x^{-1} = L_x^2 \Leftrightarrow R_x^{-1} R_x = L_x^2 R_x \Leftrightarrow I = L_x^2 R_x \Leftrightarrow y = x(xy) \cdot x \Leftrightarrow yx^{-1} = (x(xy) \cdot x)x^{-1} \Leftrightarrow yx^{-1} = x(xy)$.
 - (b) $L_x R_x = R_x^{-1} \Leftrightarrow L_x R_x^2 = I \Leftrightarrow (xy)x^2 = y \Leftrightarrow xy = yx^{-2}$.

By Theorem 1.5, $(G, \cdot)$ is a van Rees loop. The proof for left Bol loop follows by duality.

2. In a RBL, if $x^3 = e$, then $x^{-1} = x^2$. With the centrum square property, $yx^{-1} = yx^2 = x^2y$. Note that $yx^2 = x^2y \Leftrightarrow xy = yx$, hence LAP holds and $yx^{-1} = x(xy)$. So by 1., the conclusion follows. By Theorem 1.5, $(G, \cdot)$ is a van Rees loop.
3. This follows by 2.
4. $F_2 = RB$ if $R_x^{-1} = L_x^{-1}$, $L_x R_x = L_x^2$ and $R_x = L_x$.
 - (a) $R_x^{-1} = L_x^{-1} \Leftrightarrow yx = xy$.
 - (b) $L_x R_x = L_x^2 \Leftrightarrow R_x = L_x \Leftrightarrow yx = xy$.
 - (c) $R_x = L_x \Leftrightarrow yx = xy$.
5. This follows from the fact that a commutative right Bol loop is a Moufang loop.
6. $F_{12} = M_4$ if $R_x^{-1} = R_x^2$ and $R_x L_x = R_x^{-1}$.
 - (a) $R_x^{-1} = R_x^2 \Leftrightarrow I = R_x^2 R_x \Leftrightarrow y = yx^3 \Leftrightarrow e = x^3$.
 - (b) $R_x L_x = R_x^{-1} \Leftrightarrow R_x L_x R_x = I \Leftrightarrow x(yx)x = y \Leftrightarrow x(yx) = yx^{-1}$.

By Theorem 1.5, $(G, \cdot)$ is a van Rees loop.

7. This follows from the fact that an extra loop is a Moufang loop.

□

Theorem 2.6. *Let $(G, \cdot)$ be a Frute loop. Then the following are true for all $x \in G$:*

1. $|T_{(x)}| = 2$.

2. $x^{-1}yx = xyx^{-1}$.
3. $T_{(x)} \in AUM(G, \cdot)$.
4. $T_{(x)} = T_{(x^{-1})}$.
5. $(G, \cdot)$ is a A_μ -loop.
6. $(G, \cdot)$ is of exponent 2 if and only if $(xyx) \cdot (xzx) = x(yz)x$.
7. $(G, \cdot)$ is central cube if and only if $(G, \cdot)$ is commutative if and only if $(xy)^2 = x^2y^2$.

Proof. We shall make use of Lemma 2.1 and Lemma 1.1.

1.

$$\begin{aligned}
 M_4 &= (R_x^{-1}, R_x L_x, R_x), F_7^{-1} = (L_x, R_x^{-1}, L_x^{-1}) \in AUT(G, \cdot). \text{ So,} \\
 M_4 F_7^{-1} &= (R_x^{-1} L_x, L_x R_x^{-1}, T_{(x)}) \in AUT(G, \cdot). \text{ Then,} \\
 R_x^{-1} L_x &= R_{x^{-1}} L_{(x^{-1})^{-1}} = R_{x^{-1}} L_{x^{-1}}^{-1}. \text{ So,} \\
 T_{(x^{-1})} &= R_x^{-1} L_x. \text{ Also, } (L_x R_x^{-1})^{-1} = R_x L_x^{-1} = T_{(x)} \\
 &\implies (L_x R_x^{-1})^{-1} = T_{(x)} \implies L_x R_x^{-1} = T_{(x)}^{-1}.
 \end{aligned}$$

$$\text{Thus, } M_4 F_7^{-1} = (T_{(x^{-1})}, T_{(x)}^{-1}, T_{(x)}) \in AUT(G, \cdot).$$

Also,

$$\begin{aligned}
 M_4 &= (R_x^{-1}, R_x L_x, R_x), F_2^{-1} = (L_x, L_x^{-2}, L_x^{-1}) \in AUT(G, \cdot). \text{ So,} \\
 M_4 F_2^{-1} &= (R_x^{-1} L_x, R_x L_x L_x^{-2}, R_x L_x^{-1}) = (R_x^{-1} L_x, R_x L_x^{-1}, R_x L_x^{-1}) = \\
 &= (T_{(x^{-1})}, T_{(x)}, T_{(x)}) \in AUT(G, \cdot).
 \end{aligned}$$

$$\text{Then, } T_{(x)} = T_{(x)}^{-1} \implies T_{(x)}^2 = I \implies |T_{(x)}| = 2.$$

2. Let $R_x L_x^{-1} = (R_x L_x^{-1})^{-1} \Leftrightarrow R_x L_x^{-1} = L_x R_x^{-1} \Leftrightarrow y R_x L_x^{-1} = y L_x R_x^{-1} \Leftrightarrow x^{-1} y x = x y x^{-1}$.
3. From 1., $T_{(x)} = T_{(x)}^{-1}$ and by $F_5 M_1^{-1}$, $(T_{(x)}, T_{(x)}^{-1}, T_{(x)}^{-1}) = (T_{(x)}, T_{(x)}, T_{(x)}) \in AUM(G, \cdot) \implies T_{(x)}$ is an automorphism.
4. $F_{12} M_3 = (T_{(x)}^{-1}, T_{(x)}, T_{(x^{-1})}) = (L_x R_x^{-1}, T_{(x)}, R_x^{-1} L_x) = (T_{(x)}, T_{(x)}, T_{(x^{-1})}) \implies T_{(x)} = T_{(x^{-1})}$.

5. By 3.

6.

$$\begin{aligned} F_5 M_1 &= (R_x L_x, L_x R_x, L_x^3 R_x) = (R_x L_x, R_x L_x, L_x^2 L_x R_x) = \\ &= (R_x L_x, R_x L_x, R_x^2 L_x R_x) = (R_x L_x, R_x L_x, R_x R_x L_x R_x) = \\ &= (R_x L_x, R_x L_x, R_x L_x R_x^2) \in AUT(G, \cdot). \end{aligned}$$

A Frute loop $(G, \cdot)$ is of exponent 2 iff $R_x L_x \in AUM(G, \cdot)$ iff $y R_x L_x \cdot z R_x L_x = (yz) R_x L_x \Leftrightarrow (xyx) \cdot (xzx) = x(yz)x$.

$$\begin{aligned} 7. \quad x^3 \in C(G, \cdot) &\Leftrightarrow x^3 y = y x^3 \Leftrightarrow x^2 x y = y x^2 x \Leftrightarrow x^2 x y = x^2 y x \Leftrightarrow x y = y x. \\ (xy)^2 &= x^2 y^2 \Leftrightarrow (xy)^2 (xy)^{-1} = x^2 y^2 (xy)^{-1} \Leftrightarrow xy = x^2 y x^{-1} \Leftrightarrow xy = yx. \end{aligned}$$

□

Remark 2.2. *The property in 2. of Theorem 2.6 (which is equivalent to the centrum square property in a diassociative loop) is not generally true in Moufang, extra loop or group. Hence, it can be counted as a new algebraic property which distinguishes a Frute loop from a Moufang, extra loop and group. In 3 of Theorem 2.2, this property forces a group to be a Frute loop and vice versa.*

References

- [1] Adéníran J. O. and Jaiyéolá T. G. (2007), *On central loops and the central square property*, Quasigroups And Related Systems 14(2), 191–200.
- [2] Bruck R. H. (1966), *A survey of binary systems*, Springer-Verlag, Berlin-Göttingen-Heidelberg, 185pp.
- [3] Chein O., Pflugfelder H. O. and Smith, J. D. H. (1990), *Quasigroups and loops : theory and applications*, Heldermann Verlag, 568pp. 29–32.
- [4] Côté B., Harvill B., Huhn M. and Kirchman A. (2011), *Classification of generalized Bol-Moufang type*, Quasigroups and Related Systems 19, 193–206.

- [5] Dene J. and Keedwell A. D. (1974), *Latin squares and their applications*, the English University press Lts, 549pp.
- [6] Fenyves F. (1968), *Extra loops I*, Publ. Math. Debrecen, 15, 235–238.
- [7] Fenyves F. (1969), *Extra loops II*, Publ. Math. Debrecen, 16, 187–192.
- [8] Goodaire E. G., Jespers E. and Milies C. P. (1996), *Alternative loop rings*, NHMS(184), Elsevier, 387pp.
- [9] Jaiyéolá T. G. (2005), *An isotopic study of properties of central loops*, M.Sc. dissertation, University of Agriculture, Abeokuta.
- [10] Jaiyéolá T. G. (2009), *A study of new concepts in smarandache quasi-groups and loops*, ProQuest Information and Learning(ILQ), Ann Arbor, USA, 127pp.
- [11] Jaiyéolá T. G. (2009), *On the universality of central loops*, Acta Universitatis Apulensis Mathematics-Informatics, 19, 113–124.
- [12] Jaiyéolá T. G. (2015), *Generalized right central loops*, Afrika Matematika, 26(7-8), 1427–1442. DOI 10.1007/s13370-014-0297-0
- [13] Jaiyéolá T. G. and Adéníran J. O. (2006), *On the Derivatives of Central loops*, Advances in Theoretical and Applied Mathematics 1(3), 233–244.
- [14] Jaiyéolá T. G. and Adéníran J. O. (2008), *Algebraic properties of some varieties of loops*, Quasigroups And Related Systems 16(1), 37–54.
- [15] Jaiyéolá T. G. and Adéníran J. O. (2008), *On some autotopisms of non-Steiner central loops*, Journal Of Nigerian Mathematical Society, 27, 53–68.
- [16] Jaiyéolá T. G. and Adéníran J. O. (2009), *On Isotopic characterization of central Loops*, Creative Mathematics and Informatics, 18, 1, 39–45.
- [17] Jaiyéolá T. G., Adeniregun A. A. and Asiru M. A. (2017), *Finite FRUTE Loops*, J. Algebra Appl. 16(2), 1750040, 10pp. <http://dx.doi.org/10.1142/S0219498817500402>.
- [18] Kinyon M. K. and Kunen K. (2006), *Power-associative, conjugacy closed loops*, J. Algebra 304, 2, 679–711.

- [19] M. K. Kinyon and I. M. (2015), *Loops with exponent three in all isotopes*, Internat. J. Algebra Comput. 25, 7, 1159–1177.
- [20] Pflugfelder H. O. (1990), *Quasigroups and loops : Introduction*, Sigma series in Pure Math. 7, Heldermann Verlag, Berlin, 147pp.
- [21] J. D. Phillips (2019), *Generalized Bol-Moufang loop varieties—not just for breakfast!*, LOOPS 2019 Conference, Budapest University of Technology and Economics, Hungary, July 7, 2019–July 13, 2019. <https://algebra.math.bme.hu/LOOPS19/slides/phillips.pdf>
- [22] Phillips J. D. and Shcherbaco V. A. (2010), *Cheban loops*, J. Gen. Lie Theory Appl. 4, Art. ID G100501, 5 pp.
- [23] Phillips J. D. and Vojtěchovský P. (2005), *The varieties of loops of Bol-Moufang type*, Alg. Univer. 3(54), 259–383.
- [24] Phillips J. D. and Vojtěchovský P. (2005), *The varieties of quasigroups of Bol-Moufang type : An equational approach*, J. Alg. 293, 17–33.
- [25] Phillips J. D. and Vojtěchovský P. (2006), *On C-loops*, Publ. Math. Debrecen. 68, 1-2, 115–137.
- [26] Smith J. D. H. (2007), *An introduction to quasigroups and their representations*, Taylor and Francis Group, LLC.
- [27] Vasantha Kandasamy W. B. (2002), *Smarandache loops*, Department of Mathematics, Indian Institute of Technology, Madras, India, 128pp.

**ANALYTICAL SOLUTION OF AN INDUCED FIBER GRATING
RELATIVE HUMIDITY SENSOR**

Mahboubeh Dehghani Sanij and Hosein Rooholamininejad

Shahid Bahonar University, Physics Faculty

Kerman, Iran 7616914111

rooholamini@uk.ac.ir

Ali Reza Bahrampour

Sharif University of Technology, Department of Physics

Tehran, Iran 1458889694

Received July 23, 2021

Abstract

In this paper, an analytical solution is presented for a distributed sensor based on the induced Long-Period Fiber Grating (LPFG), which is designed to sense the relative moisture. The designed structure is an optical fiber coated periodically by moisture-sensitive and moisture-insensitive polymers, which is bounded by a high Young's modulus material. By absorbing the moisture, the single-mode optical fiber is deformed to an induced fiber grating that can be used as a relative humidity sensor. This solution is presented to model the symmetric and periodic designed structure. The analytical results are in a good agreement with the previously-reported numerical outcomes.

Keywords: Love's strain potential, Photo-elastic effect, Optical fiber, Relative humidity sensor.

1 Introduction

Relative Humidity (RH) is an essential factor in different industries such as food manufacturing and storage, health science, civil engineering, agriculture, biological science, and environment [1]. Furthermore, the meantime continuous monitoring of RH is necessary for intelligent systems [2]. Also, appropriate humidity levels have a significant impact on the quality of the product and can help to reduce energy consumption [3]. As a result, the design of low cost, fast response, and reversible RH sensor with excellent performance is of particular importance. In recent years, extensive investigations have been conducted on RH sensors [4]. Over the last decades, a variety of RH sensors (e.g., electrochemical methods [5], optical methods [6]) have been reported. Some limitations of these sensors include the long response time and electromagnetic interference [7]. Optical Fiber Humidity Sensors (OFHSs) have been extensively used due to their advantages, which include small size, multiplexing capability, and insensitivity to electromagnetic fields [8]. Some of the fiber-optic structures that have achieved RH sensing include long period grating [9] and tapered optical fibers [10].

Today, simulation methods and design assistants are extensively used to predict sound output to save time and improve the quality. Recently, we proposed a type of OFHS, which is based on the induced Fiber Grating in a periodic polymer-coated optical fiber structure, as a distributed RH sensor that is low-cost and easy-to-fabricate [11]. The proposed architecture is a single-mode commercial optical fiber coated by Moisture-Sensitive Polymers (MSPs) and Moisture-Insensitive Polymers (MIPs) periodically, as it is shown in Fig. 1. The structure is surrounded by a high Young modulus (E) mesh (such as stainless steel) to enhance the strain components in the optical fiber.

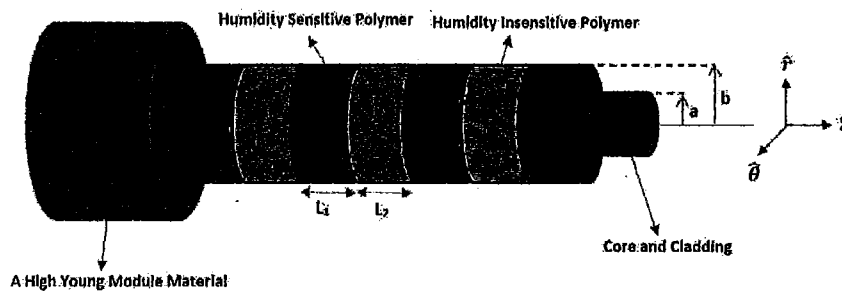


Fig. 1 The schematic diagram of the suggested RH sensor.

In the presence of humidity, MSPs swell to induce axial and radial strains. As a result, gratings can be detected in the optical fiber. Hence, this sensor can detect the amount of environmental RH at discrete locations, which are well defined by the position of the induced gratings. In this case, an Optical Time-Domain Reflectometry (OTDR) can be used to localize any water leakages, which may be distributed over several hundred meters [12] and up to more than one kilometer [11]. In this work, we focused on a semi-analytical study of finding Love's strain potential for the distributed RH sensor structure. The consequences of this semi-analytic method are in an excellent agreement with the numerical results obtained by the finite element method. If the period of the sensor structure is of the order of light wavelength, the induced grating will be an FBG, which causes the forward-to-backward mode coupling. In the long period structure, the induced grating is LPFG, which causes the core-to-cladding mode coupling. A commercial OTDR can detect both effects. The manufacturing of the suggested sensor is described in previous work [11], and it appears that the construction of the LPFG structure is cheaper and more accessible. This paper is prepared as follows: Theoretical model is presented in section 2. Finding of Love's strain potential and strain distribution in the optical fiber are introduced in Subsections 3.1 and 3.2, respectively. Numerical results can be found in section 4. The paper is finalized with some conclusion in section 5.

2 Theoretical model

The steady-state displacement vector field in the sensor structure in the presence of temperature and moisture gradients can be obtained by the well-known Lamé's equation [13]:

$$\mu \nabla^2 \vec{u} + (\lambda + \mu) \nabla (\nabla \cdot \vec{u}) = (3\lambda + 2\mu) (\nabla (\alpha \Delta T) + \nabla (\Delta R_H)) + \vec{F} \quad (1)$$

Where $\vec{u}$ is the displacement vector, λ is the Lamé's constant and μ is the modulus of rigidity. α and T are the Coefficient of Thermal Expansion (CTE) and the temperature at the observation point, respectively. R_H is the hygroscopic strain, R_{H_0} is a reference hygroscopic strain so $\Delta R_H = R_H - R_{H_0}$ and $\vec{F}$ is the body force for each unit volume. In this analysis, the temperature gradient is neglected and moisture concentration changes only at the boundaries of the structure, hence the Right Hand Side (RHS) of Eq. (1) vanishes except at the boundaries and could be approximated by Dirac delta functions, which can be replaced by suitable boundary conditions.

By introducing the vector potential, $\vec{V}$ [14], where $2\mu\vec{u} = 2(1-\nu)\nabla^2\vec{V} - \nabla(\vec{\nabla} \cdot \vec{V})$, Eq. (1) is reduced to an inhomogeneous Biharmonic equation:

$$\nabla^4 V = -\frac{\vec{F}}{1-\nu} \quad (2)$$

Where $\nu = \frac{\lambda}{2(\mu+\lambda)}$ is the Poisson's ratio.

In an axisymmetric loading scenario ($\frac{\partial}{\partial\theta} = 0$), all $\vec{V}$ components are zero except Love's strain potential, V_z ($\vec{V} = V_z \hat{e}_z$). Also, in the absence of a body force ($\vec{F} = 0$), V_z is the solution of the Biharmonic equation:

$$\nabla^4 V_z = 0 \quad (3)$$

In cylindrical coordinates, the relation between the displacement vector components and V_z are expressed as:

$$u_r = -\frac{1}{2\mu} \frac{\partial^2 V_z}{\partial r \partial z}, \quad u_\theta = 0, \quad u_z = \frac{1}{2\mu} \left[2(1-\nu) \nabla^2 V_z - \frac{\partial^2 V_z}{\partial z^2} \right] \quad (4)$$

Employing the Hook's law in the presence of the moisture ΔR_H , the stress tensor components are written [14]:

$$\sigma_{rr} = \frac{\partial}{\partial z} \left(\nu \nabla^2 - \frac{\partial^2}{\partial r^2} \right) V_z \quad (5a)$$

$$\sigma_{\theta\theta} = \frac{\partial}{\partial z} \left(\nu \nabla^2 - \frac{1}{r} \frac{\partial}{\partial r} \right) V_z \quad (5b)$$

$$\sigma_{zz} = \frac{\partial}{\partial z} \left((2-\nu) \nabla^2 - \frac{\partial^2}{\partial z^2} \right) V_z \quad (5c)$$

$$\tau_{zr} = \frac{\partial}{\partial r} \left((1-\nu) \nabla^2 - \frac{\partial^2}{\partial z^2} \right) V_z \quad (5d)$$

Continuity of the displacement vector components and the equilibrium conditions at the boundaries ($r = a, r = b, z = \frac{L_1}{2}$) of the structure are employed to obtain the solution of the Eq. (3).

The strain diagonal components of the optical fiber can be written as:

$$S_1 = \frac{\partial u_r}{\partial r}, \quad S_2 = \frac{1}{r} u_r, \quad S_3 = \frac{\partial u_z}{\partial z} \quad (6)$$

Because of the Photo-elastic effect [15], the induced strain components cause a change in the fiber refractive index, n :

$$\Delta \left(\frac{1}{n^2} \right)_i = \sum_j P_{ij} S_j \quad i, j = 1, 2, \dots, 6 \quad (7)$$

Where S_j and P_{ij} are the strain and the Photo-elastic tensor components, respectively. For an isotropic optical fiber medium, this effect has the following form [16]:

$$\frac{\Delta n(z)}{n} = -\frac{n^2}{2} [\bar{S}_1(z)(P_{11} + P_{12}) - \bar{S}_3(z)P_{12}] \quad (8)$$

Where $\bar{S}_i$ is the average value of S_i over the radial coordinate r . In order to obtain the Love's strain potential, an analytical method is introduced due to the axisymmetric and the periodic structure of the sensor. The solution of this model is presented by employing the Separation of Variables and the Fourier series method.

3 Semi-analytical method

3.1 Love's strain potential

The Separation of Variables and Fourier Series expansion are used to solve Eq. (3), so Love's strain potential can be expressed as:

$$V_z = \sum_{m=-\infty}^{+\infty} R_m(r) e^{i\frac{2m\pi}{L}z} \quad (9)$$

Where $L = L_1 + L_2$ is the period of the sensor structure and $R_m(r)$ is the Fourier expansion coefficient. By considering the normalized coordinates $\hat{r} = \frac{2\pi}{L}r$ and $\hat{z} = \frac{2\pi}{L}z$, it can be shown that:

$$\left(\frac{d^2}{d\hat{r}^2} + \frac{1}{\hat{r}}\frac{d}{d\hat{r}} - m^2\right)\left(\frac{d^2}{d\hat{r}^2} + \frac{1}{\hat{r}}\frac{d}{d\hat{r}} - m^2\right)R_m(\hat{r}) = 0 \quad (10)$$

For $m \neq 0$, $I_0(m\hat{r})$, $K_0(m\hat{r})$, $\hat{r}I_1(m\hat{r})$ and $\hat{r}K_1(m\hat{r})$ are general solutions of Eq. (10), which are denoted by $f_{im}(\hat{r})$, where $i = 1, 2, 3, 4$ respectively. The set of $\{1, \hat{r}^2, \ln \hat{r}$ and $\hat{r}^2 \ln \hat{r}\}$ are general solutions of the radial equation for $m = 0$, which are represented by $f_{i0}(\hat{r})$ where $i = 1, 2, 3, 4$. $I_n(\hat{r})$ and $K_n(\hat{r})$ are the modified Bessel functions of the first and second kinds of order n , respectively. The set of general solutions except $\ln \hat{r}$ and $K_0(m\hat{r})$ are nonsingular on the optical fiber axis. Although $\hat{r}K_1(m\hat{r})$ is nonsingular on the fiber axis, its corresponding strain component $S_{\theta\theta}$ is singular and cannot be employed in the fiber region ($r \leq a$). The Love's strain function in the k^{th} region in the periodic structure is expressed as:

$$V_z^{(k)} = \sum_{m=0}^{m=\infty} \sum_{i=1}^{i=4} A_{im}^{(k)} f_{im}(r) \cos(m\hat{z}) \quad k = 1, 2, 3, 4 \quad (11)$$

The fiber, moisture-sensitive polymer, moisture-insensitive polymer, and outer layer regions are denoted by super index $k = 1, 2, 3, 4$, respectively. It is assumed that the mechanical parameters of the core and the cladding of the optical fiber are the same.

In the fiber, $A_{30}^{(1)}$, $A_{2m}^{(1)}$ and $A_{4m}^{(1)}$ coefficients are zero for all $m \in \mathbb{N} \cup \{0\}$. The origin is located at a point on the optical fiber axis and the intermediate plane of the MSP region. In addition to the periodic symmetry, the structure is axisymmetric and $z = 0$ is a symmetric plane of the moisture sensor. Only $\cos(m\hat{z})$ appears in Eq. (9) since at $z = 0$ plane $u_z(r, 0) = 0$. The equilibrium condition in the z -direction at the interface of the MSP and MIP ($\hat{z}_1 = \frac{L_1}{L} \pi$, $a \leq r \leq b$) gives the following functional equation for $\sin(q\hat{z}_1) \neq 0$ and $p = 1, 2, 3, 4$ & $q \in \mathbb{N}$:

$$\sum_{im} (B_{im}^{(2)} + B_{im}^{(3)}) \int_a^b f_{im}(r) f_{pq}(r) dr \sin(mz_1) = \beta \Delta R_H \int_a^b f_{pq}(r) dr \quad (12)$$

Also $B_{im}^{(k)} = m^3 A_{im}^{(k)} + 2m^2(2 - \nu^{(k)}) \delta_i^{1,2} A_{i+2}^{(k)}$, where $k = 2, 3$ and If $i = j$ or $i = k$ then $\delta_i^{j,k} = 1$, otherwise it is equal to zero and β is the Coefficient of Hygroscopic Swelling (CHS) of MSP. In the system of Eq. (12), $\sin(q\hat{z}_1) = 0$ has no meaning so B_{iq} Coefficients vanish.

The continuity of u_r in the $\hat{z} = \hat{z}_1$ plane for $\sin(qz_1) \neq 0$ and $p = 1, 2, 3, 4$ & $q \in \mathbb{N}$ is reduced to:

$$\frac{A_{pq}^{(2)}}{\mu^{(2)}} = \frac{A_{pq}^{(3)}}{\mu^{(3)}} \quad (13)$$

The determinant of coefficients of Eqs. (12) and (13) is nonzero so the expansion coefficients can be obtained numerically and uniquely, and as expected, they depend on the modulus of rigidity of the MSP and MIP regions.

By employing the continuity of u_z and the tangential equilibrium condition at $\hat{z} = \hat{z}_1$ for $\cos(q\hat{z}_1) \neq 0$ and $p = 1, 2, 3, 4$ & $q \in \mathbb{N}$, one can derive:

$$\frac{1}{\mu^{(2)}} \left[2\alpha_p (1 - \nu^{(2)}) \delta_p^{1,2} A_{p+2,q}^{(2)} + q^2 A_{p,q}^{(2)} \right] = \frac{1}{\mu^{(3)}} \left[2\alpha_p (1 - \nu^{(3)}) \delta_p^{1,2} A_{p+2,q}^{(3)} + q^2 A_{p,q}^{(3)} \right] \quad (14)$$

$$\frac{1}{\mu^{(2)}} \left[\alpha_p (1 - \nu^{(2)}) \delta_p^{1,2} A_{p+2,q}^{(2)} + q^3 A_{p,q}^{(2)} \right] = \frac{1}{\mu^{(3)}} \left[\alpha_p (1 - \nu^{(3)}) \delta_p^{1,2} A_{p+2,q}^{(3)} + q^3 A_{p,q}^{(3)} \right] \quad (15)$$

It can be shown that:

$$A_{i0}^{(2)} = A_{i0}^{(3)} = 0, \quad i = 1, 2, 3, 4 \quad (16a)$$

$$A_{3m}^{(2)} = A_{3m}^{(3)} = A_{4m}^{(2)} = A_{4m}^{(3)} = 0, \quad \text{For all } m \quad (16b)$$

For a symmetric structure ($L_1 = L_2 = \frac{L}{2}$), the system of Eqs. (12) and (13) are related to the odd spatial harmonics while the homogeneous system of Eqs. (14) and (15) are presented for the even spatial harmonics. For the homogeneous system of Eqs. (12) and (13), the determinant of the coefficients is nonzero, therefore the even spatial harmonics coefficients are zero so they cannot exist in such a structure.

3.2 Strain tensor component distributions in the optical fiber region

The Fourier series expansion and the equilibrium conditions in the normal direction of the optical fiber surface ($r = a$) are used to obtain the strain tensor components in the optical fiber region, and the following equations can be derived ($n \in \mathbb{N}$):

$$A_{1n}^{(1)} f_{1n}''(a) + \left(-\nu^{(1)} f_{1n}(a) + f_{3n}''(a) \right) A_{3n}^{(1)} = \sum_{i,m} \frac{1}{n\pi} \left(D_{im}^{(3)} - D_{im}^{(2)} \right) Q_{mn} - \frac{2\varphi}{n\pi} \beta \Delta R_H \quad (17)$$

Where $\varphi = \frac{\pi L_1}{L}$, $D_{im}^{(k)} = m \left(\nu^{(k)} A_{i+2,m}^{(k)} \delta_i^{1,2} f_{im}(a) - A_{im}^{(k)} f_{im}''(a) \right)$ and $Q_{mn} = \left[-\frac{\sin(m+n)\varphi}{(m+n)} + \frac{\sin(m-n)\varphi}{(m-n)} \right]$ as $k = 1, 2$. $i = 1, 2, 3, 4$ and $m \in \mathbb{N}$. Using the continuity of the radial component of the displacement vector, one can deduce ($n \in \mathbb{N}$):

$$A_{1n}^{(1)} f_{1n}'(a) + A_{3n}^{(1)} f_{3n}'(a) = \frac{\mu^{(1)}}{n\pi} \sum_{i,m} m \left(\frac{A_{im}^{(2)}}{\mu^{(2)}} + \frac{A_{im}^{(3)}}{\mu^{(3)}} \right) f_{im}'(a) Q_{nm} \quad (18)$$

In a symmetric structure, the expansion coefficients $A_{im}^{(2)}$ and $A_{im}^{(3)}$ on the RHS of Eqs. (17) and (18) are nonzero only for odd m s and Q_{nm} s have nonzero values for even values of n , so the fundamental spatial harmonic has the following simple forms:

$$A_{11}^{(1)} = \frac{\beta \Delta R_H f_{31}'(a)}{-f_{31}'(a) f_{11}''(a) + f_{11}'(a) (-\nu^{(1)} f_{11}(a) + f_{31}''(a))} \quad (19a)$$

$$A_{31}^{(1)} = \frac{\beta \Delta R_H f_{11}'(a)}{f_{31}'(a) f_{11}''(a) - f_{11}'(a) (-\nu^{(1)} f_{11}(a) + f_{31}''(a))} \quad (19b)$$

$A_{11}^{(1)}$ and $A_{31}^{(1)}$ can be employed to determine the optical fiber refractive index distribution in the first approximation.

Only odd spatial harmonics can be excited in the regions $k=2$ and 3 (MSP and MIP) in the symmetric structure, while even spatial harmonics are excited indirectly, this effect is presented by the first terms on the RHS of Eqs. (17) and (18). In the optical fiber region ($K=1$), both odd and even spatial harmonics can be observed and are excited by the direct strain, which is represented by the second term in the RHS of Eq. (17).

4. Numerical results

The system of inhomogeneous linear Eqs. (12) and (13) can be solved by truncation and iterative method. In this method, the system of governing equations is truncated by several spatial harmonics M , and outcomes are compared with those who are given with $M-1$ spatial harmonics. A cost function is required to compare the consequences of successive steps. The relative refractive index distribution $J_M = \left(\frac{\Delta n}{n}\right)_M$ is defined as the cost function for comparing the results and the distance between the two successive cost functions in the sense of metric of $L^2[(0,L) \times (0,a)]$ space is given as the error of the numerical calculations $\varepsilon_M = \int_0^L \int_0^a (J_M - J_{M-1})^2 dz dr$.

The cost function versus the strain tensor components is given by Eq. (8).

The physical parameters of the optical fiber and polymer, which were used in the calculation, are presented in Table 1.

Table 1 Physical parameters are used in the analytical calculations.

	Radius (μm)	N	E (GPa)	ν	μ (GPa)	λ (GPa)	P_{11}	P_{12}	$\beta(\%R_H^{-1})$
Optical fiber	62.5 [17]	1.448 [18]	72 [19]	0.17 [19]	30.76	15.85	0.121 [18]	0.271[18]	-
Polyimide	104.5	-	2.45 [19]	0.41 [19]	0.86	3.95	-	-	7×10^{-5} [19]
Acrylate	104.5	-	0.028 [20]	0.38 [21]	0.01	0.03	-	-	-
Stainless	250	-	200 [22]	0.27 [22]	78.74	92.43	-	-	-

The average values of the strain tensor components $\bar{S}_{rr}$ and $\bar{S}_{zz}$ over the fiber cross-section $\bar{S}_{ii} = \frac{1}{\pi a^2} \int_0^a r S_{ii}(r, z) dr$ versus z for a period are presented in Fig.

2a and 2b, respectively. The computational error tolerance is chosen to be less than 10^{-8} , which is much smaller than the period of the recommended structure.

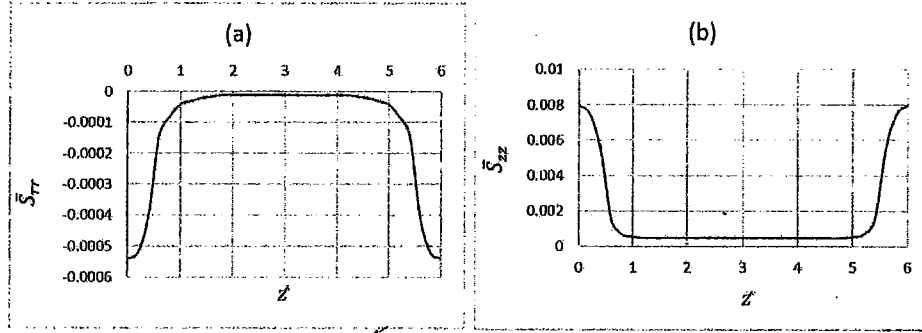


Fig. 2 Variation of the average value of the strain tensor components versus $\hat{z}$ (one period) for RH= 40% a) $\bar{S}_{rr}$ b) $\bar{S}_{zz}$.

The results show that the fundamental spatial harmonic is determined accurately and is enough for precise calculations. As expected, the maximum average value of the strain tensor components ($\bar{S}_{rr}$ and $\bar{S}_{zz}$) occurs in the middle of the MSP ($\hat{z} = 0$) in each structural period. As shown in Fig. 2, the absolute value of $\bar{S}_{zz}$ is greater than $\bar{S}_{rr}$ about one order of magnitude.

Based on Eqs. (19a) and (19b), the strain amplitudes are proportional to the RH and are shown in Fig. 3a and 3b.

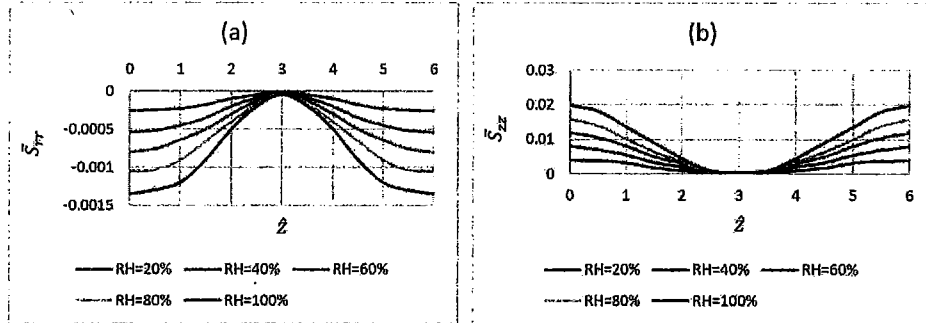


Fig. 3 Variation of the average value of the strain tensor components versus $\hat{z}$ (one period) for the different RH values a) $\bar{S}_{rr}$ b) $\bar{S}_{zz}$.

Based on the outcomes, the relative error $\varepsilon_1 = \frac{\int_0^L (\bar{s}_{11}^{(1)} - \bar{s}_{11}^{(2)})^2 dz}{\int_0^L \bar{s}_{11}^{(2)} dz}$ appears to be roughly dependent on the order of the structural period and independent of RH. The effect of the moisture distribution on the relative refractive index in the optical fiber along a period is presented in Fig. 4.

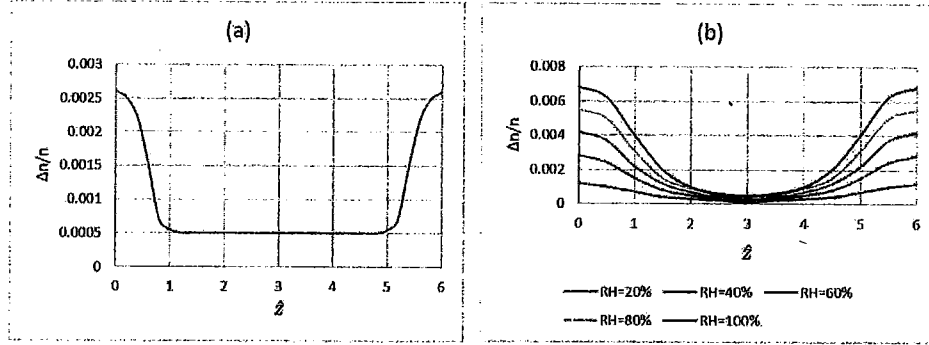


Fig. 4 Variation of the relative refractive index in the optical fiber versus $\hat{z}$, a) (one period) for RH= 40%, b) (one period) for different values of RH.

As it is expected, the amplitude of the refractive index variation is proportional to the moisture density. As the RH increases, the induced strain tensor components increase too and finally causes an increase in the relative refractive index (as shown in Figs. 3. and 4b.)

All of the results are obtained analytically, which are validated by the Finite Element Method, are compared with the numerical consequences presented in [11], and they are in a reasonable agreement.

5. Conclusions

A semi-analytic model was developed to describe the behavior of an induced fiber grating RH sensor. The method considers the influence of water on the hygroscopic polymers, induced strain, and the periodic refractive index variation in the optical fiber because of the Photo-elastic effect. For this purpose, a proper Love's strain potential was introduced to determine the strain tensor components and the average relative refractive index for one period of the structure. The outcomes from this analytical solution are in a perfect agreement with the

previous numerical consequences. Also, the correlation of sensor sensitivity with the environmental RH was shown. As a result, the proposed RH sensor is an excellent option for smart irrigation in farms, woodlands, and remote distances due to its high sensitivity and operational flexibility.

Declarations of interest: None

This research did not receive any specific grant from any funding agencies in the public, commercial, or not-for-profit sectors.

Bibliography

1. Z. Chen et al., "A sol-gel method for preparing ZnO quantum dots with strong blue emission," *J Lumin.* **131**(10), 2072 (2011) [doi:10.1016/j.jlumin.2011.05.009]
2. G. Dimitrakopoulos et al., "Intelligent transportation systems," *IEEE Veh. Technol. Mag.* **5**(1), 77–84, (2010) [doi:10.1109/MVT.2009.935537]
3. M. Schirmer et al., "Impact of air humidity in industrial heating processes on selected quality attributes of bread rolls," *J. Food Eng.* **105**(4), 647–655 (2011) [doi:10.1016/j.jfoodeng.2011.03.020]
4. X. Wang et al., "Humidity sensing properties of Pd²⁺ doped ZnO nanotetrapods," *APPL SURF SCI.* **253**(6), 3168 (2007) [doi:10.1016/j.apsusc.2006.07.033]
5. S. L. Gao et al., "Glass fibers with carbon nanotube networks as multifunctional sensors," *Adv. Funct. Mater.* **20**(12), 1885–1893, (2010) [doi:10.1002/adfm.201000283]
6. M. V. Fuke et al., "Optical humidity sensing characteristics of ag-polyaniline nanocomposite," *IEEE Sensors J.* **9**(6), 648–653 (2009) [doi: 10.1109/JSEN.2009.2020662]
7. T. L. Yeo et al., "Fibre-optic sensor technologies for humidity and moisture measurement," *Sens. Actuators A, Phys.* **144**(2), 280–295 (2008) [doi: 10.1016/j.sna.2008.01.017]
8. F. J. Arregui et al., "Optical fiber humidity sensor using a nano Fabry–Perot cavity formed by the ionic self-assembly method," *Sens. Actuators B, Chem.* **59**(1), 54–59 (1999) [doi: 10.1016/S0925-4005(99)00232-4]

9. M.Y. Fu et al., "Fiber-optic humidity sensor based on an air-gap long-period fiber grating," *Opt. Rev.* **18**(1), 93–95 (2011) [doi: 10.1007/s10043-011-0038-7]
10. J. M. Corres et al., "Design of humidity sensors based on tapered optical fibers," *J. Lightw. Technol.* **24**(11), 4329–4336 (2006).
11. M. Dehghani Sanij et al., "A Proposal for Distributed Humidity Sensor based on the Induced LPFG in A Periodic Polymer Coated Fiber Structure," *Opt. Laser. Technol.* **117**, 126-133 (2019) [doi: 10.1016/j.optlastec.2019.04.019]
12. A. MacLean et al., "Detection of hydrocarbon fuel spills using distributed fiber optic sensor", *Sens. Actuators A.* **109**(1-2) 60–67 (2003) [doi: 10.1016/j.sna.2003.09.007]
13. L. D. Landau, and E. M. Lifshitz, *Theory of Elasticity*, 3rd ed., Pergamon Press, Oxford, UK, (1986).
14. M. H. Sadd, *Elasticity: theory, applications, and numerics*, Academic Press, (2009).
15. A. Yariv, *Quantum electronics*, 3rd ed., John Wiley & Sons, (1989).
16. A. Bertholds et al., "Deformation of single-mode optical fibers under static longitudinal stress," *J Lightwave Technol.* **5**(7), 895-900 (1987) [doi: 10.1109/JLT.1987.1075583]
17. "Diameter of an Optical Fiber - The Physics Factbook - Hypertextbook", <https://hypertextbook.com/facts/1997/LaurenBoyd.shtml>
18. T. A. Ali et al., "Design and performance investigation of a highly accurate apodized fiber Bragg grating-based strain sensor in single and quasi-distributed systems," *Appl Optics.* **54**(16), 5243-5251 (2015) [doi: 10.1364/AO.54.005243]
19. Q. Chen et al., "Fiber Bragg gratings and their applications as temperature and humidity sensors," *J at Mol Opt Phys.* 235-260 (2008).
20. S. C. Her et al., "Effect of coating on the strain transfer of optical fiber sensors," *Sensors.* **11**(7), 6926-6941 (2011) [doi: 10.3390/s110706926]
21. M. R. Lin et al., "Measuring the interfacial shear strength of thin polymer coatings on glass," *J Mater Res.* **5**(5), 1110-1117 (1990) [doi:10.1557/JMR.1990.1110]
22. "Material Data Book" (Cambridge University Engineering Department, 2003) <http://www-mdp.eng.cam.ac.uk/web/library/enginfo/cueddatabooks/materials.pdf>.

HALIDON RINGS AND THEIR APPLICATIONS

A. Telveenus

Kingston University of London International Study Centre
Stable Block, Kingston Hill Campus
KT2 7LB, UK
t.fernandezantony@kingston.ac.uk

Received September 12, 2021

Abstract

Halidon rings are rings with a unit element, containing a primitive m^{th} root of unity and m is invertible in the ring. The field of complex numbers is a halidon ring with any index $m \geq 1$. This article examines different applications of halidon rings. The main application is the extension of Maschke's theorem. In representation theory, Maschke's theorem has an important role in studying the irreducible subrepresentations of a given group representation and this study is related to a finite field of characteristic which does not divide the order of the given finite group or the field of real or complex numbers. The second application is the computational aspects of halidon rings and group rings which enable us to verify Maschke's theorem. Some computer codes have been developed to establish the existence of halidon rings which are not fields and the computation of units, involutions and idempotents in both halidon rings and halidon group rings. The third application of halidon rings is in solving Rososhek's problem related to some cryptosystems. The applications in Bilinear forms and Discrete Fourier Transform (DFT) with two computer codes developed to calculate DFT and inverse DFT have also been discussed.

Keywords 1 *Maschke's theorem; Primitive m^{th} roots of unity; halidon rings; Rososhek's problem, bilinear forms; Discrete Fourier Transform.*

AMS 1 *16S34, 20C05, 68W30*

Former Prof. & Head, Dept. of Mathematics, Fatima Mata National College, University of Kerala, Kollam, S. India. Supported by no grants from any sources.

1 Introduction

In 1940, the famous celebrated mathematician Graham Higman published a theorem [3] in group algebra which is valid only for a field or an integral domain with some specific conditions. In 1999, the author noticed that this theorem can be extended to a rich class of rings called halidon rings[9]. In complex analysis, $|z| = 1$ is the set of all points on a circle with centre at the origin and radius 1. The solutions of $z^n = 1$, which are usually called the n^{th} roots of unity, which can be computed by DeMoivre's theorem, will form a regular polygon with vertices as the solutions. As $n \rightarrow \infty$ this regular polygon will become a unit circle. This is the ordinary concept of n^{th} of unity in the field of complex numbers. For a ring, we need to think differently.

A primitive m^{th} root of unity in a ring with unit element is completely different from that of in a field, because of the presence of nonzero zero divisors. So we need a separate definition for a primitive m^{th} root of unity. An element ω in a ring R is called a *primitive m^{th} root* if m is the least positive integer such that $\omega^m = 1$ and

$$\begin{aligned} \sum_{r=0}^{m-1} \omega^{r(i-j)} &= m, \quad i = j \pmod{m} \\ &= 0, \quad i \neq j \pmod{m}. \end{aligned}$$

More explicitly,

$$\begin{aligned} 1 + \omega^r + (\omega^r)^2 + (\omega^r)^3 + (\omega^r)^4 + \dots + (\omega^r)^{m-1} &= m, \quad r = 0 \\ &= 0, \quad 0 < r \leq m - 1. \end{aligned}$$

A ring R with unity is called a *halidon* ring with index m if there is a primitive m^{th} root of unity and m is invertible in R . The ring of integers is a halidon ring with index $m = 1$ and $\omega = 1$. The halidon ring with index 1 is usually called a *trivial* halidon ring. The field of real numbers is a halidon ring with index $m = 2$ and $\omega = -1$. The field $\mathbb{Q}(i) = \{a + ib | a, b \in \mathbb{Q}\}$ is

a halidon ring with $\omega = i$ and $m = 4$. $\mathbb{Z}_{65}$ is an example of a halidon ring with index 4 and $\omega = 8$ which is not a field. In general $\mathbb{Z}_{4r^2+1}$ is a halidon ring with index 4 and $\omega = 2r$ for each integer $r > 0$. $\mathbb{Z}_p$ is a halidon ring with index $p - 1$ for every prime p . Interestingly, $\mathbb{Z}_{p^k}$ is also a halidon ring with same index for any integer $k > 0$ and it is not a field if $k > 1$. Note that if ω is a primitive m^{th} root of unity, then ω^{-1} is also a primitive m^{th} root of unity.

2 Preliminary results

Let $U(R)$ and $ZD(R)$ denote the unit group of R and the set of zero divisors in R respectively. Clearly, they are disjoint sets for a finite commutative halidon ring R .

Lemma 1 *A finite commutative ring R with unity is a halidon ring with index m if and only if there is a primitive m^{th} root of unity ω such that $m, \omega^r - 1 \in U(R)$; the unit group of R for all $r = 1, \dots, m - 1$. If m is a prime number it is enough to have $m, \omega - 1 \in U(R)$.*

Proof 1 *The proof follows from the fact that $(\omega^r - 1)(1 + \omega^r + (\omega^r)^2 + (\omega^r)^3 + (\omega^r)^4 + \dots + (\omega^r)^{m-1}) = \omega^{rm} - 1 = 0$.*

Proposition 1 *Let R be a finite commutative halidon ring with index m . Then $R = U(R) \cup ZD(R)$ with $U(R) \cap ZD(R) = \{\}$; the empty set.*

Proof 2 *Since R is finite and m is invertible in R , the proof is evident.*

The next theorem will give an improved necessary and sufficient conditions for a ring to be a halidon ring.

Theorem 1 *A finite commutative ring R with unity is a halidon ring with index m if and only if there is a primitive m^{th} root of unity ω such that $m, \omega^d - 1 \in U(R)$; the unit group of R for all divisors d of m and $d < m$.*

Proof 3 *If R is a finite commutative halidon ring with index m , then it is evident that there is a primitive m^{th} root of unity ω such that $m, \omega^d - 1 \in$*

$U(R)$; the unit group of R for all divisor d of m .

Conversely, assume that there is a primitive m^{th} root of unity ω such that $m, \omega^d - 1 \in U(R)$; the unit group of R for all divisor d of m . We would like to show that $\omega^r - 1 \in U(R)$, for $r = 1, 2, 3, \dots, m - 1$. Let g be the greatest common divisor of r and m . Then there are integers u and v such that $ur + vm = g$. Using the well known geometric series, we have

$$(p - 1)(1 + p + p^2 + \dots + p^{k-1}) = p^k - 1.$$

Put $p = \omega^r$ and $k = u$. Then we get $(\omega^r - 1).a = \omega^{ru} - 1$ for some $a \in R$. This means that $(\omega^r - 1)$ divides $\omega^{ru} - 1 = \omega^{ru}.\omega^{vm} - 1 = \omega^{ru+vm} - 1 = \omega^g - 1$. Now we can choose a divisor d of m such that g divides d . Let $p = \omega^g$ and $k = \frac{d}{g}$. Thus we have

$$(\omega^g - 1).b = \omega^d - 1$$

for some $b \in R$. If $(\omega^g - 1).c = 0$, multiplying by b , we get $(\omega^d - 1).c = 0$. Since $(\omega^d - 1) \in U(R)$, $c = 0$. Therefore $(\omega^g - 1)$ is not a zero divisor. Since R is finite and using proposition 1, we get $(\omega^g - 1) \in U(R)$. Also, $(\omega^r - 1)$ divides $\omega^g - 1$. Therefore $(\omega^r - 1)$ is a unit in R . Thus we have $(\omega^r - 1)$ is a unit in R for $r = 1, 2, 3, \dots, m - 1$. By lemma 1, R is a halidon ring with index m .

The following results are stated without proof. For proofs, refer to [9] and [10].

Proposition 2 Let R be a finite commutative halidon ring with index m . Then m divides the number of nonzero zero divisors in R .

Proposition 3 Let R be a commutative halidon ring with index m and let $k > 1$ be a divisor of m . Then R is also a halidon ring with index k .

Proposition 4 Let I be an ideal of a halidon ring with index m . Then R/I is also a halidon with same index m .

The cardinality of a finite non-trivial commutative halidon ring is given by the following proposition.

Proposition 5 Let R be a finite commutative halidon ring with index m . Then $|R| \equiv 1 \pmod{m}$.

Example 1 Let $R = Z_{p^k}$ where p is an odd prime. Then R is a halidon ring with index $m = p-1$ and $p^k = (1+p+p^2+p^3+\dots+p^{k-1})(p-1)+1 \equiv 1 \pmod{m}$. $\therefore |R| \equiv 1 \pmod{m}$.

Proposition 6 Let R be a finite commutative halidon ring with index $m > 1$ such that $U(R) = \langle \omega \rangle$, where $\langle \omega \rangle$ is the cyclic group generated by ω ; a primitive m^{th} root of unity. Then

1. $R = T \oplus L$, where T is a subfield of R and L is a subspace of R as a vector space over T ,
2. R is semisimple.

The next theorem will give the necessary and sufficient conditions for a non-trivial halidon ring to become a field.

Theorem 2 A ring R is a finite field if and only if R is a finite commutative halidon ring with index $m > 1$ such that $U(R) = \langle \omega \rangle$; where $\langle \omega \rangle$ is the cyclic group generated by ω ; a primitive m^{th} root of unity.

Example 2 Let $R = Z_{25}$. Then $U(R) = \langle 2 \rangle$ and $2^{20} = 1$. R is not a halidon ring as the index 20 is not invertible in R . However, $R = Z_5$ is a halidon ring with index 4, $\omega = 2$ and $U(R) = \langle 2 \rangle$ which is also a field.

Let

$$u = \sum_{i=1}^m \alpha_i g_i$$

be an element in the group algebra RG and let

$$\lambda_r = \sum_{i=1}^m \alpha_{m-i+2} (\omega^{(i-1)})^{(r-1)}$$

where $\omega \in R$ is a primitive m^{th} root of unity. Then u is said to be depending on $\lambda_1, \lambda_2, \dots, \lambda_m$.

Proposition 7 *Let S be a subring with unity of a halidon ring R with index m and let $G = \langle g \rangle = \{g_1 = 1, g_2 = g, \dots, g_m = g^{m-1}\}$ be a cyclic group of order m generated by g . Let*

$$u = \sum_{i=1}^m \alpha_i g_i \in U(RG) \cap SG$$

be depending on $\lambda_1, \lambda_2, \dots, \lambda_m$. Then $u^{-1} \in SG$ if and only if $\lambda = \lambda_1 \lambda_2 \dots \lambda_m$ is invertible in S .

The next theorem is about the existence of units in integral group rings which is an important area of study in group rings or group algebras.

Theorem 3 *Let $\omega \in \mathbb{C}$ be a complex primitive m^{th} root of unity and let $G = \langle g \rangle = \{g_1 = 1, g_2 = g, \dots, g_m = g^{m-1}\}$ be a cyclic group of order m generated by g . Let*

$$u = \sum_{i=1}^m \alpha_i g_i \in \mathbb{C}G$$

be depending on $\lambda_1, \lambda_2, \dots, \lambda_m$. Let

$$\lambda_i^* = \prod_{r=1, r \neq i}^m \lambda_r$$

and

$$\lambda = \prod_{r=1}^m \lambda_r$$

Then

$$u = \sum_{i=1}^m \alpha_i g_i \in U(\mathbb{Z}G)$$

if and only if $\lambda = \pm 1$. If $\lambda_m^{-1} = f(\omega)$; a polynomial function of ω , then $u^{-1} = f(g)$.

Remark 1 *When we use the formula $u^{-1} = f(g)$, ensure that the use of*

$$\sum_{r=0}^{m-1} \omega^r = 0$$

should be avoided in the calculation of λ_i or λ in order to make the behaviour of ω exactly same as that of g . For an example see [9].

Theorem 4 *Let R be a commutative halidon ring with index m and let G be a cyclic group of order m . Then $RG \cong R^m$ as R -algebras.*

Theorem 5 (Higman's Theorem [3], [5]) *Let R be a commutative halidon ring with index m and let G be an finite abelian group of order n with exponent m and n is a unit in R . Then $RG \cong R^n$ as R -algebras.*

3 Main Result- Maschke's Theorem

In this section, we discuss the characters of a group over halidon rings and Maschke's Theorem. Usually, the character of a group is defined over a real field $\mathbb{R}$ or a complex field $\mathbb{C}$. But, here we define character of a group over a halidon ring which need not be a field. Since the field of complex numbers is a halidon ring with any index greater than 1, all the properties of characters over halidon rings will automatically satisfied over the field of complex numbers. Now we are looking into those properties of characters of a group over a complex field which are also true over halidon rings.

Let R be a commutative halidon ring with index m and let G be a finite group of order n with exponent m such that n is invertible in R . A homomorphism $\rho : G \rightarrow GL(k, R)$ is defined as a *representation* of G over R of *degree* k , where $GL(k, R)$ is the general linear group of invertible matrices of order k over R . The *character* of G is defined as a homomorphism $\chi : G \rightarrow R$ such that $\chi(g) = \text{tr}(\rho(g))$ for $\forall g \in G$ where $\text{tr}(\rho(g))$ is the trace of the matrix $\rho(g)$. A representation is *faithful* if it is injective. When $k = 1$, we call the character χ as *linear* character and it is actually a homomorphism $\chi : G \rightarrow u(R)$. In the standard definition, by a *linear* character χ of G , mean a homomorphism $\chi : G \rightarrow \mathbb{C} - \{0\}$. If $R = \mathbb{C}$, then $U(R) = \mathbb{C} - \{0\}$. So the linear characters are precisely $\Gamma^{[r]}$. Thus we have the following theorem which is already known to be true for linear characters of a group over $\mathbb{C}$.

Theorem 6 Let R be a commutative halidon ring with index m and let G be a group of order n and exponent m such that n is invertible in R . Let G^* be the set of homomorphisms $\Gamma^{[s]}$ of G into $U(R)$, which are given by (*). Then G^* is a group under the product $\Gamma^{[s]}\Gamma^{[t]} = \Gamma^{[s+t]}$ and $G^* \cong G$.

Proof 4 Refer to [10] for the proof.

Suppose that $\rho : G \rightarrow GL(k, R)$ is a representation of G over R . Write $V = R^k$, the module of all row vectors $(\lambda_1, \lambda_2, \dots, \lambda_k)$ with each $\lambda_i \in R$. For all $v \in R$ and $g \in G$, the matrix product

$$v\rho(g),$$

of the row vector v with the matrix $\rho(g)$ is a row vector in V . With the multiplication $vg = v\rho(g)$, V becomes an RG -module. Refer to [2].

The next theorem is the Maschke's Theorem for a cyclic group over a halidon ring.

Theorem 7 Let G be a finite cyclic group of order m and let R be a commutative halidon ring with index m . Let $V = R^m$ be an RG -module. Then there are m irreducible RG -submodules $U_1, U_2, \dots, U_m$ such that $V = U_1 \oplus U_2 \oplus \dots \oplus U_m$.

Proof 5 Let ρ be the regular representation of $G = \langle g | g^m = 1 \rangle$. Then

$$\rho(g) = \text{cirulant}(0, 0, 0, \dots, 1) = \begin{pmatrix} 0 & 0 & 0 \dots & 0 & 1 \\ 1 & 0 & 0 \dots & 0 & 0 \\ \cdot & \cdot & \dots & \cdot & \cdot \\ 0 & 0 & 0 \dots & 1 & 0 \end{pmatrix}$$

is a square matrix of order m and each row is obtained by moving one position right and wrapped around of the row above. The eigen values are

$$1, \omega, \omega^2, \dots, \omega^{m-1},$$

where ω is a primitive m^{th} root of unity and with corresponding eigen vectors $(1, 1, \dots, 1), (1, \omega, \omega^2, \dots, \omega^{m-1}), (1, \omega^2, (\omega^2)^2, \dots, (\omega^{m-1})^2), \dots, (1, \omega^{m-1}, (\omega^{m-1})^2, \dots, (\omega^{m-1})^{m-1})$.

Let $U_r = \text{span}\{(1, \omega^{r-1}, (\omega^{r-1})^2, \dots, (\omega^{r-1})^{m-1})\}$. Then any element u_r of U_r can be taken as $\lambda(1, \omega^{r-1}, (\omega^{r-1})^2, \dots, (\omega^{r-1})^{m-1})$ for some $\lambda \in R$. Therefore

$$\begin{aligned} ug &= u\rho(g) \\ &= \lambda(1, \omega^{r-1}, (\omega^{r-1})^2, \dots, (\omega^{r-1})^{m-1})\text{cirulant}(0, 0, 0, \dots, 1) \\ &= \lambda\omega^{r-1}(1, \omega^{r-1}, (\omega^{r-1})^2, \dots, (\omega^{r-1})^{m-1}) \in U_r. \end{aligned}$$

This means that U_r is an RG -submodule of V for each $r = 1, 2, 3, \dots, m$. We define $\pi_r : V \rightarrow V$ by

$$\pi_r(v) = u_r \in U_r.$$

Then $\pi_r^2 = \pi_r$ and therefore $V = U_1 \oplus U_2 \oplus \dots \oplus U_m$.

Corollary 1 Let G be a finite cyclic group of order k and let R be a commutative halidon ring with index m . Let $V = R^k$ be an RG -module where $k \mid m$. Then there are k irreducible RG -submodules $U_1, U_2, \dots, U_k$ such that $V = U_1 \oplus U_2 \oplus \dots \oplus U_k$.

Proof 6 Since $k \mid m$, we can take $m=ck$. Then $\omega_1 = \omega^c$ is a primitive k^{th} root of unity. Applying the above theorem, the result follows.

Theorem 8 (Mascheke's Theorem) Let G be a finite group of order n with exponent m , let R be a commutative halidon ring with index m and n is invertible in R . Let $V = R^m$ be an RG -module. If U is an RG -submodule of V , then there is an RG -submodule W such that $V = U \oplus W$.

Proof 7 First choose any submodule W_0 of V such that $V = U \oplus W_0$. Since V is a free module with rank m , we can find a basis $\{v_1, \dots, v_p\}$ of U . Next we have to show that this basis can be extended to a basis $\{v_1, \dots, v_p, v_{p+1}, \dots, v_m\}$ of V . Let $v_{p+1} \notin \text{span}\{v_1, \dots, v_p\}$. Suppose that

$$\alpha_1 v_1 + \alpha_2 v_2 + \dots + \alpha_p v_p + \alpha_{p+1} v_{p+1} = 0.$$

Then

$$\alpha_{p+1}v_{p+1} = -\alpha_1v_1 - \alpha_2v_2 - \dots - \alpha_pv_p$$

If $\alpha_{p+1} = 0$, then $v_1, \dots, v_p, v_{p+1}$ are linearly independent.

If $\alpha_{p+1} \in U(R)$; the unit group of R , then $v_{p+1} \in \text{span}\{v_1, \dots, v_p\}$, which is a contradiction. So $\alpha_{p+1} \notin U(R)$.

If $\alpha_{p+1} \neq 0 \in ZD(R)$; the set of zero divisors of R , then there exists a $\beta_{p+1} \neq 0 \in ZD(R)$ such that $\alpha_{p+1}\beta_{p+1} = 0$.

$$\Rightarrow -\beta_{p+1}\alpha_1v_1 - \beta_{p+1}\alpha_2v_2 - \dots - \beta_{p+1}\alpha_pv_p = 0$$

$\Rightarrow \beta_{p+1}\alpha_i = 0$ for all $i = 1, 2, 3, \dots, p$. Since the above is true for all $i = 1, 2, 3, \dots, p$, β_{p+1} must be zero. This is a contradiction as $\beta_{p+1} \neq 0$. Therefore α_{p+1} must be zero. So $v_1, \dots, v_p, v_{p+1}$ are linearly independent. Continuing like this we can extend a basis $\{v_1, \dots, v_p\}$ of U to a basis $\{v_1, \dots, v_p, v_{p+1}, \dots, v_m\}$ of V . Then $W_0 = \text{span}\{v_{p+1}, \dots, v_m\}$.

Rest of the proof is in line with [2]. Now for all $v \in V$ there exist unique vectors $u \in U$ and $w \in W_0$ such that $v = u + w$. We define $\phi : V \rightarrow V$ by setting $\phi(v) = u$. Recall from algebra that if $V = U \oplus W$, and if we define $\pi : V \rightarrow V$ by

$$\pi(u + w) = u \quad \text{for all } u \in U, w \in W$$

then π is an endomorphism of V . Moreover, $\text{Im}(\pi) = U$, $\text{Ker}(\pi) = W$ and $\pi^2 = \pi$. With this in mind we see that ϕ is a projection of V with kernel W_0 and image U . Our aim is to modify the projection ϕ to create an RG -homomorphism from $V \rightarrow V$ with image U .

Define $\tau : V \rightarrow V$ by

$$\tau(v) = \frac{1}{n} \sum_{g \in G} g^{-1} \phi(gv), \quad v \in V$$

Then τ is an endomorphism of V and $\text{Im}(\tau) \subseteq U$. Now we will show that τ is an RG -homomorphism. For $v \in V$ and $x \in G$ we have

$$\tau(xv) = \frac{1}{n} \sum_{g \in G} g^{-1} \phi(gxv)$$

As g runs through the elements of G , so does $h = gx$. Thus we have

$$\begin{aligned}\tau(xv) &= \frac{1}{n} \sum_{h \in G} xh^{-1}\phi(hv) \\ &= \frac{1}{n} x \left(\sum_{h \in G} h^{-1}\phi(hv) \right) \\ &= x\tau(v)\end{aligned}$$

Thus τ is an RG -homomorphism.

It remains to show that τ is a projection with image U . To show that τ is a projection it suffices to demonstrate that $\tau^2 = \tau$. Note that given $u \in U$ and $g \in G$, we have $gu \in U$, so $\phi(gu) = gu$. Using this we see that:

$$\begin{aligned}\tau(u) &= \frac{1}{n} \sum_{g \in G} g^{-1}\phi(gu) \\ &= \frac{1}{n} \sum_{g \in G} g^{-1}gu \\ &= \frac{1}{n} \sum_{g \in G} u \\ &= u\end{aligned}$$

Now let $v \in V$. Then $\tau(v) \in U$, so we have $\tau(\tau(v)) = \tau(v)$. We have shown that $\tau^2 = \tau$.

In [2], the authors have stated the Maschke's theorem for vector spaces over the field of real numbers $\mathbb{R}$ or complex numbers $\mathbb{C}$ and provided an example where Maschke's theorem can fail (see chapter 7) if the field is not a $\mathbb{R}$ or $\mathbb{C}$. In the light of the theorem 8, we can still have a vector space over the field $\mathbb{Z}_p$; which is a halidon ring with index $m = p - 1$ for prime p . By theorem 2, there is a primitive m^{th} root of unity ω such that $U(\mathbb{Z}_p) = \langle \omega \rangle$. Let $G = C_m = \langle a : a^m = 1 \rangle$ and let $R = \mathbb{Z}_p$. Note that we cannot take G as $C_p = \langle a : a^p = 1 \rangle$ as $|G| = p$ has no multiplicative inverse in $\mathbb{Z}_p$. Let $V = R^2$ and let $\{v_1, v_2\}$ be the standard basis for V . We define $\sigma : G \longrightarrow GL(2, R)$ by $\sigma(a^j) = \begin{pmatrix} \omega^j & 0 \\ 0 & \omega^j \end{pmatrix}$ for $j = 1, 2, 3, \dots, m..$ Clearly

σ is a representation of G . Also, $U = \text{span}\{v_1\}$ is an RG -submodule of V . Define $W = \text{span}\{v_1 + v_2\}$, which is also an RG -submodule of V . Any element v in V can be written as $v = (\alpha_1 - \alpha_2)v_1 + \alpha_2(v_1 + v_2)$ for some $\alpha_1, \alpha_2 \in R$. If $x \in U \cap W$, then $x \in U$ and $x \in W$. So $x = \lambda_1 v_1 = (\lambda_1, 0)$ and $x = \lambda_2(v_1 + v_2) = (\lambda_2, \lambda_2)$ for some $\lambda_1, \lambda_2 \in R$. This implies $x = (0, 0)$ and hence $V = U \oplus W$ as desired.

Definition 1 Let R be a commutative halidon ring with index $m > 2$ and let S_n be the symmetric group on n symbols such that $|S_n| = m$. Let $S_n = \{g_1, g_2, g_3, \dots, g_m\}$ be in some order and let $\{e_{g_1}, e_{g_2}, e_{g_3}, \dots, e_{g_m}\}$ be the standard basis for $V = R^m$. Define $\rho(g)(h) = e_{gh}$ for all $g, h \in S_n$. This is called the **permutation representation** of S_n .

Example 3 Let us order the elements of S_3 as follows:

$$S_3 = \{g_1 = \text{id}, g_2 = (1, 2), g_3 = (1, 3), g_4 = (2, 3), g_5 = (1, 2, 3), g_6 = (1, 3, 2)\}.$$

Then the composition table is given as below.

	g_1	g_2	g_3	g_4	g_5	g_6
g_1	g_1	g_2	g_3	g_4	g_5	g_6
g_2	g_2	g_1	g_5	g_6	g_3	g_4
g_3	g_3	g_6	g_1	g_5	g_4	g_2
g_4	g_4	g_5	g_6	g_1	g_2	g_3
g_5	g_5	g_4	g_2	g_3	g_6	g_1
g_6	g_6	g_3	g_4	g_2	g_1	g_5

Let R be a halidon ring with index $m=6$ and $V = R^6$ (for example, $R = \mathbb{Z}_{49}$). Let $\{e_{g_1}, e_{g_2}, e_{g_3}, \dots, e_{g_6}\}$ be the standard basis for V . The representation ρ is given by $\rho(g_i)g_j = e_{g_i g_j}$. Using the composition table, for example, we can see that

$$\rho(g_3) = \begin{pmatrix} 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \end{pmatrix}$$

Let $W_0 = \text{span}\{e_{g_1}, e_{g_2}, e_{g_3}, e_{g_4}, e_{g_5}\}$ and $U = \text{span}\{e_{g_1} + e_{g_2} + e_{g_3} + e_{g_4} + e_{g_5} + e_{g_6}\}$. Then clearly $V = W_0 \oplus U$. We define a projection $\phi(e_{g_i}) = 0$, for $i = 1, 2, 3, 4, 5$ and $\phi(e_{g_6}) = e_{g_1} + e_{g_2} + e_{g_3} + e_{g_4} + e_{g_5} + e_{g_6}$. From the proof of Maschke's Theorem, we have $\tau(e_{g_i}) = \frac{1}{6}(e_{g_1} + e_{g_2} + e_{g_3} + e_{g_4} + e_{g_5} + e_{g_6})$ for all $i = 1, 2, 3, 4, 5, 6$. Let $W = \text{Ker } \tau = \text{span}\{e_{g_1} - e_{g_2}, e_{g_2} - e_{g_3}, e_{g_3} - e_{g_4}, e_{g_4} - e_{g_5}, e_{g_5} - e_{g_6}\}$. Then $wg \in W$ for all $w \in W$ and $g \in S_3$. Therefore W is an RS_3 submodule and $V = U \oplus W$ as expected from the Maschke's Theorem.

4 Rososhek's problem

The Rososhek's problem is a problem related to a cryptosystem using group rings [8]. Let R be a commutative ring and G be a group. We say that an automorphism $\psi : RG \rightarrow RG$ is *standard* if it is defined by some ring automorphism $\alpha : R \rightarrow R$ and by a group automorphism $\sigma : G \rightarrow G$, so that

$$\psi(x) = \sum_{g \in G} \alpha(a_g) \sigma(g)$$

for every

$$x = \sum_{g \in G} a_g g \in RG$$

Rososhek's problem: For which finite commutative rings R and finite groups G does the group ring RG have standard automorphisms only?

We refer to group rings RG possessing just standard automorphisms as *automorphically rigid*, and the problem then consists in defining finite *automorphically rigid* group rings. In [8], the author has proved the following theorem for a finite field:

Theorem 9 *Let K be a finite field of characteristic p and G a finite group. A group algebra KG is automorphically rigid if and only if one of the following conditions holds:*

1. G is a trivial group, i.e., $G = e$;

2. G is a cyclic group of odd prime order q , i.e., $G = C_q$, $q = 2$, and $K = F_p$ is a prime field of characteristic p , with p a primitive root modulo q ;
3. G is a direct product of an order 2 cyclic group and a cyclic group C_q of odd prime order $q = 2$, i.e., $G = C_2 \times C_q$, with 2 a primitive root modulo q , and $K = F_2$ is a two-element field;
4. G is a permutation group on three symbols, i.e., $G = S_3$, and $K = F_2$ is a two-element field.

Still, the question remains unanswered for a finite commutative ring which is not a field.

Proposition 8 Let $R = \frac{\mathbb{Z}_n[X]}{(X^2 - 1)}$. Then the number of automorphisms of R , $|AutR|$ is given by

$$\begin{aligned} |AutR| &= 2 \text{ if } n = p^s \text{ where } s \geq 1 \text{ is an integer and } p \text{ is an odd prime number} \\ &= 2^k \text{ if } n = p_1^{e_1} p_2^{e_2} p_3^{e_3} \dots p_k^{e_k} \text{ with prime numbers } 2 < p_1 < p_2 < \dots < p_k. \end{aligned}$$

Proof 8 This proof is somewhat similar to example 2 in [7]. Let x be the image of X in R . Any element in R can be uniquely written as $ax + b$ with $a, b \in \mathbb{Z}_n$. Let $\sigma \in AutR$. Then $\sigma(a) = a$ for every $a \in \mathbb{Z}_n$. Therefore $\sigma(x) = ax + b$ for some $a, b \in \mathbb{Z}_n$. Since σ is an automorphism, there exists an element $px + q$ with $p, q \in \mathbb{Z}_n$ such that $x = \sigma(px + q) = p\sigma(x) + q = p(ax + b) + q$. then we get $pa = 1$ and so a must be a unit in $\mathbb{Z}_n$. Further, if $\sigma(x) = ax + b$ with $a \in U(\mathbb{Z}_n)$, we must also have $0 = \sigma(x^2 - 1) = \sigma(x^2) - 1 = (ax + b)^2 - 1 = a^2x^2 + 2abx + b^2 - 1 = a^2(x^2 - 1) + 2abx + a^2 + b^2 - 1 = 2abx + a^2 + b^2 - 1$.

Since n is odd, $2ab = 0 \implies b = 0$ as $a \in U(\mathbb{Z}_n)$. This implies $a^2 = 1$. Therefore $|AutR| = \text{no. of involutions in } \mathbb{Z}_n$. But, the number of involutions in $\mathbb{Z}_n$ clearly follows the statement in the proposition. Programme-3 mentioned below is useful to compute involutions in $\mathbb{Z}_n$.

If $\mathbb{Z}_n$ is halidon ring with index m , then so is $\mathbb{Z}_n[X]$. By proposition 4, $\frac{\mathbb{Z}_n[X]}{(X^2 - 1)}$ is also a halidon ring with index m .

Proposition 9 *Let $R = \frac{\mathbb{Z}_n[X]}{(X^2 - 1)}$ be a halidon ring with index m and let $G = C_m$ be a cyclic group of order m . If $m! = 2^k \times \phi(m)$ for some positive integer k , then RG is automorphically rigid.*

Proof 9 *Clearly R is not a field. By theorem 5, $RG \cong R^m$. So $|AutRG| = |AutR^m|$. But, $AutR^m$ is just the collection of automorphisms which permute the positions of the elements of R^m . Thus we have $|AutR^m| = m!$. By proposition 8, we have $|AutR| = 2^k$ for some positive integer k . So $m! = 2^k \times \phi(m)$ implies $|AutRG| = |AugR| \times |AugG|$ and therefore RG is automorphically rigid.*

The only solution to the above proposition is $m = 2$. So one of the solutions (there may have other solutions) to the Rososhek's problem is given by $R = \frac{\mathbb{Z}_{p^s}[X]}{(X^2 - 1)}$ where p is an odd prime, $s \geq 1$ is an integer and $\omega = p^s - 1 = -1 \text{ mod } p^s \in \mathbb{Z}_{p^s}$ is a primitive m^{th} root of unity and $G = C_2$.

5 The computational aspects of halidon rings and halidon group rings

The main purpose this section is to verify Maschke's Theorem using some computer codes. The computer programme-5, is very useful to verify the Maschke's theorem for cyclic group. Throughout this section, let $R = \mathbb{Z}_n$ be a halidon ring with index m and primitive m^{th} root of unity ω . Let $G = \langle g \rangle = \{g_1 = 1, g_2 = g, \dots, g_m = g^{m-1}\}$ be a cyclic group of order m generated by g . We study the computational aspects of finding halidon rings for any integer $n > 2$ and computing the units and idempotents in the halidon group ring RG based on the related theorems.

Definition 2 Let $p_1, p_2, p_3, \dots, p_k$ be odd primes and let $\phi(x)$ be the Euler's totient function. We define the halidon function

$$\psi(n) = \begin{cases} \gcd\{\phi(p_1^{e_1}), \phi(p_2^{e_2}), \phi(p_3^{e_3}), \dots, \phi(p_k^{e_k})\}, & n = p_1^{e_1} p_2^{e_2} p_3^{e_3} \dots p_k^{e_k} \\ 1, & n \text{ is even} \end{cases}$$

Proposition 10 Let n be as in 2. Then the halidon function

$$\psi(n) = \gcd\{p_1 - 1, p_2 - 1, p_3 - 1, \dots, p_k - 1\},$$

which is independent of the exponents $e_1, e_2, e_3, \dots, e_k$.

Proof 10 The proof follows immediately from the fact that $p_1, p_2, p_3, \dots, p_k$ are distinct primes.

It is well-known that the carmichael function $\lambda(n)$ is the exponent of $U(\mathbb{Z}_n)$. The proof of the following proposition is evident.

Proposition 11 If $\lambda(n)$ is the carmichael function, then

1. $\psi(n)$ divides $\lambda(n)$,
2. $\psi(n^k) = \psi(n)$ if n is odd,
3. $\psi(p_1 p_2 p_3 \dots p_s) = \psi(p_1^{d_1} p_2^{d_2} p_3^{d_3} \dots p_s^{d_s})$ if each integer $d_i > 0$ for $i = 1, 2, 3, \dots, s$.

I have developed 5 computer programme codes in c++ (Microsoft Visual Studio 2019) based on the theorems 1, 11 and 2 programmes for Discrete Fourier Transforms. The programme codes are included in the appendix.

The computer programme-1 can be used to find a halidon ring Z_n of given order $n \geq 1$. The author would like to provide its algorithm as follows:

ALGORITHM for Programme-1

Input: n .

Output: Z_n is a trivial halidon ring or not.

1. If n is even, then Z_n is a trivial halidon ring.

2. Else

for $i=1,2,\dots, n-1$

for $j=1,2,3,\dots,n-1$ do compute $i * j \bmod n$

if $i*j \bmod n=1$, $w \leftarrow i$

3. for $i=1,2,3,\dots, n-1$ do compute w^i

4. if $w^i \bmod n = 1$, $m \leftarrow i$

5. compute divisors d of m and $d < m$

6. compute $w^d - 1$ and if $w^d - 1 = 1 \bmod n$ for all d , then Z_n is a nontrivial halidon ring with index m .

End

There are infinitely many halidon rings which are not fields. For example, using the programme-1, we can see that:

1. Z_{49} is halidon ring with index $m = 6$ and $\omega = 19$,
2. Z_{2001} is a trivial halidon ring with index $m = 2$ and $\omega = 2000$,
3. Z_{2501} is halidon ring with index $m = 20$ and $\omega = 8$ or 2493 ,
4. Z_{3601} is halidon ring with index $m = 12$ and $\omega = 1350$ or 2528 ,
5. Z_{10001} is halidon ring with index $m = 8$ and $\omega = 10$ or 9220 ,
6. Z_{100001} is halidon ring with index $m = 10$ and $\omega = 26364$ or 73728 (running time 35 minutes).

By running the same programme several times for different values of n , the author has come to the conclusion of the following conjecture.

Conjecture 1 *If $R = \mathbb{Z}_n$ and $n = p_1^{e_1} p_2^{e_2} p_3^{e_3} \dots p_k^{e_k}$ with primes $p_1 < p_2 < p_3 < \dots < p_k$ including 2, then R is a halidon ring with maximal index $m_{max} = \psi(n)$.*

Theorem 10 *Let*

$$u = \sum_{i=1}^m \alpha_i g_i \in U(RG)$$

be depending on $\lambda_1, \lambda_2, \dots, \lambda_m$. Let

$$v = \sum_{i=1}^m \beta_i g_i$$

be the multiplicative inverse of u in RG . Then

$$\beta_i = \frac{1}{m} \sum_{r=1}^m \lambda_r^{-1} (\omega^{i-1})^{r-1}.$$

The computer programme-2 can be used to test whether a given element u in RG is a unit or not. If it is a unit, then the programme will give the multiplicative inverse v in RG .

Input: $n = 121, m = 10, m^{-1} = 109, \omega = 94, a[1] = 62, a[2] = 21, a[3] = 22, a[4] = 85, a[5] = 81, a[6] = 95, a[7] = 24, a[8] = 30, a[9] = 1, a[10] = 65$

Output: The multiplicative inverse of $a = 62 + 21g + 22g^2 + 85g^3 + 81g^4 + 95g^5 + 24g^6 + 30g^7 + g^8 + 65g^9$ is $b = 102 + 68g + 34g^2 + 61g^3 + 73g^4 + 54g^5 + 102g^6 + 109g^7 + 18g^8 + 455g^9$.

Input: $n = 121, m = 10, m^{-1} = 109, \omega = 94, a[1] = 72, a[2] = 71, a[3] = 89, a[4] = 48, a[5] = 54, a[6] = 0, a[7] = 2, a[8] = 105, a[9] = 25, a[10] = 19$

Output: The multiplicative inverse of $a = 72 + 71g + 89g^2 + 48g^3 + 54g^4 + 0g^5 + 2g^6 + 105g^7 + 25g^8 + 19g^9$ is $b = 72 + 71g + 89g^2 + 48g^3 + 54g^4 + 0g^5 + 2g^6 + 105g^7 + 25g^8 + 19g^9$, which is an involution.

Input: $n = 121, m = 10, m^{-1} = 109, \omega = 94, a[1] = 5, a[2] = 7, a[3] = 2, a[4] = 40, a[5] = 22, a[6] = 90, a[7] = 20, a[8] = 25, a[9] = 10, a[10] = 55$

Output: The element $a = 5 + 7g + 2g^2 + 40g^3 + 22g^4 + 90g^5 + 20g^6 + 25g^7 + 10g^8 + 56g^9$ has no multiplicative inverse.

A direct calculation shows that all outputs are correct.

Theorem 11 Let

$$u = \sum_{i=1}^m \alpha_i g_i \in RG$$

be depending on $\lambda_1, \lambda_2, \dots, \lambda_m$. Then

1. $u \in U(RG)$ if and only if each $\lambda_i \in U(R)$,

2. $u \in E(RG)$ if and only if each $\lambda_i \in E(R)$, where $E(RG)$ is the set of idempotents in RG .

More over, $|U(RG)| = |U(R)|^{|G|}$ and $|E(RG)| = |E(R)|^{|G|}$.

Proof 11 The proof follows from the isomorphism $\rho(u) = (\lambda_1, \lambda_2, \dots, \lambda_m)$ from RG onto R^m . This is the isomorphism used to prove theorem 4.

In order to find a unit element or an involution or an idempotent in R , we can use the programme-3.

Input: $n=25$

Output: Involutions are 1 and 24.

Idempotents are 0 and 1.

The units and their inverses are (1, 1), (2, 13), (3, 17), (4, 19), (6, 21), (7, 18), (8, 22), (9, 14), (11, 16), (12, 23), (13, 2), (14, 10), (16, 11), (17, 3), (18, 7), (9, 4), (21, 5), (22, 20), (23, 12) and (24, 24).

After finding the units and involutions in R , using the programme-4, we can compute the units and involutions in RG .

Input: $n = 25, m = 4, m^{-1} = 19, \omega = 7, l[1] = 7, l[2] = 3, l[3] = 13, l[4] = 21, l1[1] = 18, l1[2] = 17, l1[3] = 2, l1[4] = 5$

Output: The multiplicative inverse of $a = 11 + 17g + 24g^2 + 5g^3$ is $b = 23 + 12g^2 + 8g^3$.

Input: $n = 25, m = 4, m^{-1} = 19, \omega = 7, l[1] = 1, l[2] = 24, l[3] = 24, l[4] = 1, l1[1] = 1, l1[2] = 24, l1[3] = 24, l1[4] = 1$

Output: The multiplicative inverse of $a = 22g + 4g^3$ is $b = 22g + 4g^3$, which is an involution.

All outputs can be verified through direct calculations.

After finding the idempotents in R , using the programme-5, we can compute the idempotents in RG .

Input: $n = 49, m = 6, m^{-1} = 41, \omega = 19, l[1] = 1, l[2] = 0, l[3] = 0, l[4] = 0, l[5] = 0, l[6] = 0$

Output: $e_1 = 41 + 41g + 41g^2 + 41g^3 + 41g^4 + 41g^5$

Input: $n = 49, m = 6, m^{-1} = 41, \omega = 19, l[1] = 0, l[2] = 1, l[3] = 0, l[4] = 0, l[5] = 0, l[6] = 0$

Output: $e_2 = 41 + 44g + 3g^2 + 8g^3 + 5g^4 + 46g^5$

Input: $n = 49, m = 6, m^{-1} = 41, \omega = 19, l[1] = 0, l[2] = 0, l[3] = 1, l[4] = 0, l[5] = 0, l[6] = 0$

Output: $e_3 = 41 + 3g + 5g^2 + 41g^3 + 3g^4 + 5g^5$

Input: $n = 49, m = 6, m^{-1} = 41, \omega = 19, l[1] = 0, l[2] = 0, l[3] = 0, l[4] = 1, l[5] = 0, l[6] = 0$

Output: $e_4 = 41 + 8g + 41g^2 + 8g^3 + 41g^4 + 8g^5$

Input: $n = 49, m = 6, m^{-1} = 41, \omega = 19, l[1] = 0, l[2] = 0, l[3] = 0, l[4] = 0, l[5] = 1, l[6] = 0$

Output: $e_5 = 41 + 5g + 3g^2 + 41g^3 + 5g^4 + 3g^5$

Input: $n = 49, m = 6, m^{-1} = 41, \omega = 19, l[1] = 0, l[2] = 0, l[3] = 0, l[4] = 0, l[5] = 0, l[6] = 1$

Output: $e_6 = 41 + 46g + 5g^2 + 8g^3 + 3g^4 + 44g^5$

Clearly e_1, e_2, e_3, e_4, e_5 and e_6 are orthogonal idempotents such that $e_1 + e_2 + e_3 + e_4 + e_5 + e_6 = 1$. Therefore $\mathbb{Z}_{49}G = U_1 \oplus U_2 \oplus U_3 \oplus U_4 \oplus U_5 \oplus U_6$ where $U_1 = \text{span}\{41 + 41g + 41g^2 + 41g^3 + 41g^4 + 41g^5\} = \text{span}\{1 + g + g^2 + g^3 + g^4 + g^5\}$, $U_2 = \text{span}\{41 + 44g + 3g^2 + 8g^3 + 5g^4 + 46g^5\} = \text{span}\{1 + \omega g + \omega^2 g^2 + \omega^3 g^3 + \omega^4 g^4 + \omega^5 g^5\}$,

$U_3 = \text{span}\{41 + 3g + 5g^2 + 41g^3 + 3g^4 + 5g^5\} = \text{span}\{1 + (\omega)^2 g + (\omega^2)^2 g^2 + (\omega^2)^3 g^3 + (\omega^2)^4 g^4 + (\omega^2)^5 g^5\}$,

$U_4 = \text{span}\{41 + 8g + 41g^2 + 8g^3 + 41g^4 + 8g^5\} = \text{span}\{1 + (\omega)^3 g + (\omega^3)^2 g^2 + (\omega^3)^3 g^3 + (\omega^3)^4 g^4 + (\omega^3)^5 g^5\}$,

$U_5 = \text{span}\{41 + 5g + 3g^2 + 41g^3 + 5g^4 + 3g^5\} = \text{span}\{1 + (\omega)^4 g + (\omega^4)^2 g^2 + (\omega^4)^3 g^3 + (\omega^4)^4 g^4 + (\omega^4)^5 g^5\}$,

$U_6 = \text{span}\{41 + 46g + 5g^2 + 8g^3 + 3g^4 + 44g^5\} = \text{span}\{1 + (\omega)^5 g + (\omega^5)^2 g^2 + (\omega^5)^3 g^3 + (\omega^5)^4 g^4 + (\omega^5)^5 g^5\}$, after multiplying by 6, the inverse of 41. This confirms the theorem 7.

Input: $n = 65, m = 4, m^{-1} = 49, \omega = 8, l[1] = 1, l[2] = 26, l[3] = 40, l[4] = 26$

Output: The idempotent in $\mathbb{Z}_{65}G$ is $e = 7 + 39g + 46g^2 + 39g^3$.

A direct calculation verifies that all outputs are correct.

6 Bilinear Forms and Circulant Matrices

Let ring R be a commutative halidon ring with index m and primitive m^{th} root of unity ω . Let G be a cyclic group of order m , generated by g . We define $g_i = g^{i-1}$. $\therefore g_i g_j = g_{i+j-1}$; $i = 1, 2, 3, \dots, m$. By the extension theorem of Higman, we have $RG \cong R^m$ as R -algebras and the isomorphism ρ is given by

$$\rho \left(\sum_{i=1}^m \alpha_i g_i \right) = (\lambda_1, \lambda_2, \lambda_3, \dots, \lambda_m)$$

where

$$\lambda_i = \sum_{r=1}^m \alpha_{m-r+1} (\omega^{i-1})^{r-1}.$$

Since $\{g_i\}$ is an R -basis for RG , $\{\rho(g_i)\}$ is a basis for R^m and

$$\begin{aligned} s_1 &= \rho(g_1) = (1, 1, 1, \dots, 1), \\ s_2 &= \rho(g_2) = (1, \omega^{m-1}, (\omega^{m-1})^2, \dots, (\omega^{m-1})^{m-1}), \\ s_3 &= \rho(g_3) = (1, \omega^{m-2}, (\omega^{m-2})^2, \dots, (\omega^{m-2})^{m-1}), \end{aligned}$$

.....,

$$s_m = \rho(g_m) = (1, \omega, \omega^2, \dots, \omega^{m-1}).$$

Let $\{e_i\}$ be the standard basis in R^m . Then

$$\begin{aligned} s_1 &= e_1 + e_2 + e_3 + \dots + e_m, \\ s_2 &= e_1 + \omega^{m-1}e_2 + (\omega^{m-1})^2e_3 + \dots + (\omega^{m-1})^{m-1}e_m, \\ s_3 &= e_1 + \omega^{m-2}e_2 + (\omega^{m-2})^2e_3 + \dots + (\omega^{m-2})^{m-1}e_m, \end{aligned}$$

.....,

$$s_m = e_1 + \omega e_2 + \omega^2 e_3 + \dots + \omega^{m-1} e_m.$$

This gives

$$\begin{pmatrix} s_1 \\ s_2 \\ s_3 \\ \dots \\ s_m \end{pmatrix} = \begin{pmatrix} 1 & 1 & 1 & \dots & 1 \\ 1 & \omega^{m-1} & (\omega^{m-1})^2 & \dots & (\omega^{m-1})^{m-1} \\ 1 & \omega^{m-2} & (\omega^{m-2})^2 & \dots & (\omega^{m-2})^{m-1} \\ \dots & \dots & \dots & \dots & \dots \\ 1 & \omega & (\omega)^2 & \dots & (\omega^{m-1}) \end{pmatrix} \begin{pmatrix} e_1 \\ e_2 \\ e_3 \\ \dots \\ e_m \end{pmatrix}$$

$$s^T = \Phi^* e^T$$

$$\therefore e^T = \frac{1}{m} \Phi s^T$$

where

$$\Phi = \begin{pmatrix} 1 & 1 & 1 & \dots & 1 \\ 1 & \omega & \omega^2 & \dots & \omega^{m-1} \\ 1 & \omega^2 & (\omega^2)^2 & \dots & (\omega^2)^{m-1} \\ \cdot & \cdot & \cdot & \dots & \cdot \\ \cdot & \cdot & \cdot & \dots & \cdot \\ \cdot & \cdot & \cdot & \dots & \cdot \\ 1 & \omega^{m-1} & (\omega^{m-1})^2 & \dots & (\omega^{m-1})^{m-1} \end{pmatrix}$$

and Φ^* is the Φ conjugate transposed[1]. Thus we have the following theorem.

Theorem 12 Let ring R be commutative halidon ring with index m and primitive m^{th} root of unity ω . Let G be a cyclic group of order m , generated by g . We define $g_i = g^{i-1}$; $i = 1, 2, 3, \dots, m$ and let $\{s_i\}$ be the image of $\{g_i\}$ under the isomorphism $RG \cong R^m$ and let $\{e_i\}$ be the standard basis for R^n . Then $s^T = \Phi^* e^T$ or $e^T = \frac{1}{m} \Phi s^T$.

For each $u = (u_1, u_2, u_3, \dots, u_m) \in R^m$, we define $C_u = circu(u_1, u_2, u_3, \dots, u_m)$. Also, we define $f_u : R^m \times R^m \rightarrow R$ by

$$f_u(x, y) = \langle x, y \rangle_u = x C_u y^T$$

for every $x = (x_1, x_2, x_3, \dots, x_m), y = (y_1, y_2, y_3, \dots, y_m) \in R^m$. We adopt some standard definitions of bilinear form for $\langle x, y \rangle_u$. $\langle x, y \rangle_u$ is said to be *symmetric* if $\langle x, y \rangle_u = \langle y, x \rangle_u$ for every $x, y \in R^m$. It is said to be *skewsymmetric* if $\langle x, y \rangle_u = -\langle y, x \rangle_u$ for every $x, y \in R^m$. $\langle x, y \rangle_u$ is said to be *alternating* if $\langle x, x \rangle_u = 0$ for every $x \in R^m$ [6].

Theorem 13 f_u is a bilinear form and

$$\begin{aligned} \langle s_i, s_j \rangle_u &= m(u_1 + u_2 \omega^{i-1} + u_3 (\omega^{i-1})^2 + \dots + u_m (\omega^{i-1})^{m-1}), \\ &\text{if } i + j = 2 \pmod{m} \\ &= 0 \quad \text{otherwise.} \end{aligned}$$

Proof 12 It is clear that f_u is a bilinear form.

$$\begin{aligned} \langle e_i, e_j \rangle_u &= e_i C_u e_j^T = u_{j-i+1} \quad \text{if } i \leq j \\ &= u_{m+j-i+1} \quad \text{if } i > j. \end{aligned}$$

$$\begin{aligned}
\langle s_i, s_j \rangle_u &= \langle e_1 + \omega^{m-i+1}e_2 + (\omega^{m-i+1})^2e_3 + \dots + (\omega^{m-i+1})^{m-1}e_m, \\
&e_1 + \omega^{m-j+1}e_2 + (\omega^{m-j+1})^2e_3 + \dots + (\omega^{m-j+1})^{m-1}e_m \rangle_u \\
&= (u_1 + \omega^{m-j+1}u_2 + (\omega^{m-j+1})^2u_3 + \dots + (\omega^{m-j+1})^{m-1}u_m) \\
&+ (\omega^{m-i+1})(u_m + \omega^{m-j+1}u_1 + (\omega^{m-j+1})^2u_2 + \dots + (\omega^{m-j+1})^{m-1}u_{m-1}) \\
&+ (\omega^{m-i+1})^2(u_{m-1} + \omega^{m-j+1}u_m + (\omega^{m-j+1})^2u_1 + \dots + (\omega^{m-j+1})^{m-2}u_{m-1}) \\
&+ \dots + (\omega^{m-i+1})^{m-1}(u_2 + \omega^{m-j+1}u_3 + (\omega^{m-j+1})^2u_4 + \dots + (\omega^{m-j+1})^{m-1}u_1) \\
&= u_1(1 + \omega^{2m-i-j+2} + (\omega^{2m-i-j+2})^2 + \dots + (\omega^{2m-i-j+2})^{m-1}) \\
&+ u_2\omega^{m-i+1}(1 + \omega^{2m-i-j+2} + (\omega^{2m-i-j+2})^2 + \dots + (\omega^{2m-i-j+2})^{m-1}) \\
&+ u_3(\omega^{m-i+1})^2(1 + \omega^{2m-i-j+2} + (\omega^{2m-i-j+2})^2 + \dots + (\omega^{2m-i-j+2})^{m-1}) \\
&+ \dots + u_m(\omega^{m-i+1})^{m-1}(1 + \omega^{2m-i-j+2} + (\omega^{2m-i-j+2})^2 + \dots + (\omega^{2m-i-j+2})^{m-1}) \\
&= (1 + \omega^{2m-i-j+2} + (\omega^{2m-i-j+2})^2 + \dots + (\omega^{2m-i-j+2})^{m-1}) \\
&(u_1 + u_2\omega^{m-j+1} + u_3(\omega^{m-j+1})^2 + \dots + u_m(\omega^{m-j+1})^{m-1})
\end{aligned}$$

$$\begin{aligned}
\omega^{2m-i-j+2} &= 1 \quad \text{if } i+j = 2 \pmod{m} \\
&\neq 1 \quad \text{otherwise}
\end{aligned}$$

$$\begin{aligned}
\therefore \langle s_i, s_j \rangle_u &= m(u_1 + u_2\omega^{i-1} + u_3(\omega^{i-1})^2 + \dots + u_m) \quad \text{if } i+j = 2 \pmod{m} \\
&= 0 \quad \text{otherwise.}
\end{aligned}$$

Hence the proof.

Corollary 2 $\langle s_i, s_j \rangle_u = 0$ for all $i, j \in \{1, 2, 3, \dots, m\}$ if and only if $u = 0$.

Proof 13 If $u = 0$, there is nothing to prove.

By theorem 13, $\langle s_i, s_j \rangle_u = 0$ for all i, j other than $i+j = 2 \pmod{m}$. So it is enough to consider $\langle s_i, s_j \rangle_u = 0$ for $i+j = 2 \pmod{m}$. Since m is invertible in R , $\langle s_i, s_j \rangle_u = 0$ for $i+j = 2 \pmod{m}$ implies

$$\begin{array}{rcl} u_1 + u_2 + u_3 + \dots + u_m & = & 0 \\ u_1 + u_2\omega + u_3(\omega)^2 + \dots + u_m(\omega)^{m-1} & = & 0 \\ u_1 + u_2\omega^2 + u_3(\omega^2)^2 + \dots + u_m(\omega^2)^{m-1} & = & 0 \\ \vdots & & \vdots \\ u_1 + u_2\omega^{m-1} + u_3(\omega^{m-1})^2 + \dots + u_m(\omega^{m-1})^{m-1} & = & 0 \end{array}$$

This can be put into the matrix form $\Phi u^T = 0$. Since Φ^{-1} exists, $u^T = 0$ and therefore $u = 0$.

We write $x \perp y$ if $\langle x, y \rangle_u = 0$. We define $(R^m)^\perp = \{x \in R^m \mid \langle x, y \rangle_u = 0 \text{ for all } y \in R^m\}$. We say that $\langle x, y \rangle_u$ is *nondegenerate* if $(R^m)^\perp = \{0\}$.

Corollary 3 $\langle x, y \rangle_u$ is a nondegenerate bilinear form if $\langle s_i, s_j \rangle_u \in U(R)$ for all i and j such that $i + j = 2 \pmod{m}$.

Proof 14 $\langle x, y \rangle_u = \sum_{i,j} x_i y_j \langle s_i, s_j \rangle_u = \sum_{i+j=2 \bmod(m)} x_i y_j \langle s_i, s_j \rangle_u$
by 13.

Therefore $\langle x, y \rangle_u = x_1 y_1 \langle s_1, s_1 \rangle_u + x_2 y_m \langle s_2, s_m \rangle_u +$

$$x_3y_{m-1} < s_3, s_{m-1} >_u + \dots + x_my_2 < s_m, s_2 >_u$$

$$\langle x, y \rangle_u = 0 \implies x_1 y_1 < s_1, s_1 \rangle_u + x_2 y_m < s_2, s_m \rangle_u +$$

$$x_3y_{m-1} < s_3, s_{m-1} >_u + \dots + x_my_2 < s_m, s_2 >_u = 0$$

$$\Rightarrow \left(x_1 < s_1, s_1 >_u \quad x_2 < s_2, s_m >_u \quad x_3 < s_3, s_{m-1} >_u \quad \dots \quad x_m < s_m, s_2 >_u \right)$$

$$\begin{pmatrix} y_1 \\ y_m \\ y_{m1} \\ \vdots \\ y_2 \end{pmatrix} = 0. \text{ Since this is true for all } y = (y_1, y_2, y_3, \dots, y_m),$$

$$\left(\begin{array}{ccccccc} x_1 < s_1, s_1 >_u & x_2 < s_2, s_m >_u & x_3 < s_3, s_{m-1} >_u & & x_m < s_m, s_2 >_u \end{array} \right) \\ = (0, 0, \dots, 0)$$

$$\Rightarrow x_1 < s_1, s_1 >_u = 0, x_2 < s_2, s_m >_u = 0, x_3 < s_3, s_{m-1} >_u = 0..$$

$$x_m < s_m, s_2 >_u = 0$$

$$x_1 = x_2 = x_3 = \dots = x_m = 0 \text{ only when } \langle s_i, s_j \rangle_u \in U(R) \text{ for } i + j =$$

$2 \pmod{m}$.

Thus $(R^m)^\perp = \{0\}$ and therefore $\langle x, y \rangle_u$ is a nondegenerate bilinear form.

Corollary 4 Let $\langle x, y \rangle_u$ be a nondegenerate bilinear form. Then $M = (\langle s_i, s_j \rangle)$ is an invertible matrix of order m .

Proof 15 By theorem 13, the matrix M can be written as

$$M = \begin{pmatrix} \langle s_1, s_1 \rangle_u & 0 & 0 & \dots & 0 & 0 \\ 0 & 0 & 0 & \dots & 0 & \langle s_2, s_m \rangle_u \\ 0 & 0 & 0 & \dots & \langle s_3, s_{m-1} \rangle_u & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & \langle s_m, s_2 \rangle_u & 0 & \dots & 0 & 0 \end{pmatrix}$$

Clearly $D = \det M = \pm \langle s_1, s_1 \rangle_u \langle s_2, s_m \rangle_u \langle s_2, s_{m-1} \rangle_u \dots \langle s_m, s_2 \rangle_u$ and the sign is depending on m . By corollary 3, $D \in U(R)$. So M^{-1} exists and M^{-1} is given by

$$M^{-1} = \begin{pmatrix} \langle s_1, s_1 \rangle_u^{-1} & 0 & 0 & \dots & 0 & 0 \\ 0 & 0 & 0 & \dots & 0 & \langle s_m, s_2 \rangle_u^{-1} \\ 0 & 0 & 0 & \dots & \langle s_{m-1}, s_3 \rangle_u^{-1} & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & \langle s_2, s_m \rangle_u^{-1} & 0 & \dots & 0 & 0 \end{pmatrix}.$$

Corollary 5 Let $R = Z_n$ be the ring integers modulo n . It is a halidon ring with maximum index $m_{\max} = \psi(n)$; where $\psi(n)$ is the halidon function. Then the number of nondegenerate bilinear forms $\langle x, y \rangle_u$ is $\phi(n)^{\psi(n)}$.

Proof 16 By 3, $\langle x, y \rangle_u$ is nondegenerate if and only if $\langle s_i, s_j \rangle_u \in U(R)$ for all i and j such that $i + j = 2 \pmod{m}$. Here $|U(R)| = \phi(n)$ and $m = \psi(n)$. Therefore $|\langle x, y \rangle_u| = \phi(n)^{\psi(n)}$.

Theorem 14 Let $C = \{C_u | u = (u_1, u_2, u_3, \dots, u_m) \in R^m\}$ and let G be as in theorem 12. Then C is an R -algebra.

Proof 17 Let $u = (u_1, u_2, u_3, \dots, u_m), v = (v_1, v_2, v_3, \dots, v_m) \in R^m$ be any two elements in R . Since $RG \cong R^m$, we can identify the elements u and v as $\sum_{i=1}^m \alpha_i g_i$ and $\sum_{i=1}^m \beta_i g_i$ respectively, where

$$u_i = \sum_{r=1}^m \alpha_{m-r+2} (\omega^{i-1})^{r-1}.$$

and

$$v_i = \sum_{r=1}^m \beta_{m-r+2} (\omega^{i-1})^{r-1}.$$

Since R is a halidon ring with index m and ω is a primitive m^{th} root of unity, the circulant matrix C_u can be written as

$$C_u = \frac{1}{m} \Phi \Lambda_u \Phi^*,$$

where

$$\Lambda_u = \text{diag}(\lambda_1, \lambda_2, \lambda_3, \dots, \lambda_m)$$

such that

$$\lambda_i = \sum_{r=1}^m u_i (\omega^{(i-1)})^{(r-1)}$$

and Φ^* is the conjugate transposed of Φ [1] and $\frac{1}{m} \Phi \Phi^* = I = \frac{1}{m} \Phi^* \Phi$. Clearly $\Lambda_u \Lambda_v = \Lambda_{uv}$.

$$\begin{aligned} \therefore C_{uv} &= \frac{1}{m} \Phi \Lambda_{uv} \Phi^* \\ &= \frac{1}{m} \Phi \Lambda_u \Lambda_v \Phi^* \\ &= \frac{1}{m} \Phi \Lambda_u \frac{1}{m} \Phi^* \Phi \Lambda_v \Phi^* \\ &= \left(\frac{1}{m} \Phi \Lambda_u \Phi^* \right) \left(\frac{1}{m} \Phi \Lambda_v \Phi^* \right) \\ &= C_u C_v \end{aligned}$$

We define $h : R^m \rightarrow C$ by $h(u) = C_u$; which is clearly an algebra isomorphism. $\therefore R^m \cong C$. And hence the theorem.

Theorem 15 Let $B = \{ \langle x, y \rangle_u \mid \langle x, y \rangle_u = x C_u y^T, \text{ for each } u \in R^m, x, y \in R^m \}$. Then B is an R -module.

Proof 18 Let $\alpha \in R$ be any element in R . Then $\langle x, y \rangle_{u+v} = \langle x, y \rangle_u + \langle x, y \rangle_v$ and $\langle x, y \rangle_{\alpha u} = \alpha \langle x, y \rangle_u$. Therefore B is an R -module.

7 Discrete Fourier Transforms

In this section, we deal with the ring of polynomials over a halidon ring which has an application in Discrete Fourier Transforms [4]. Throughout this section, let R be a finite commutative halidon ring with index m and $R[x]$ denotes the ring of polynomials degree less than m over R .

Definition 3 [4] Let $\omega \in R$ be a primitive m^{th} root of unity in R and let $f(x) = \sum_{j=0}^{m-1} f_j x^j \in R[x]$ with its coefficients vector $(f_0, f_1, f_2, \dots, f_{m-1}) \in R^m$. The **Discrete Fourier Transform (DFT)** is a map

$$DFT_{\omega} : R[x] \rightarrow R^m$$

defined by

$$DFT_{\omega}(f(x)) = (f_0(1), f_1(\omega), f_2(\omega^2), \dots, f_{m-1}(\omega^{m-1})).$$

Remark 2 Clearly DFT_{ω} is a R -linear map as $DFT_{\omega}(af(x) + bg(x)) = aDFT_{\omega}(f(x)) + bDFT_{\omega}(g(x))$ for all $a, b \in R$. Also, if $R = \mathbb{C}$, the field of complex numbers, then $\omega = \cos(\frac{2\pi}{m}) + i\sin(\frac{2\pi}{m}) = e^{i\frac{2\pi}{m}}$ and the Fourier series will become the ordinary series of sin and cos functions.

Definition 4 [4] The **convolution** of $f(x) = \sum_{j=0}^{m-1} f_j x^j$ and $g(x) = \sum_{k=0}^{m-1} g_k x^k$ in $R[x]$ is defined by $h(x) = f(x) * g(x) = \sum_{l=0}^{m-1} h_l x^l \in R[x]$ where $h_l = \sum_{j+k=l \text{ mod } m} f_j g_k = \sum_{j=0}^{m-1} f_j g_{l-j}$ for $0 \leq l < m$.

The notion of convolution is equivalent to polynomial multiples in the ring $R[x]/\langle x^m - 1 \rangle$. The l^{th} coefficient of the product $f(x)g(x)$ is $\sum_{j+k=l \text{ mod } m} f_j g_k$ and hence

$$f(x) * g(x) = f(x)g(x) \text{ mod}(x^m - 1).$$

Proposition 12 [4] For polynomials $f(x), g(x) \in R[x]$, $DFT_\omega(f(x)*g(x)) = DFT_\omega(f(x)).DFT_\omega(g(x))$, where $.$ denotes the pointwise multiplication of vectors.

Proof 19 $f(x) * g(x) = f(x)g(x) + q(x)(x^m - 1)$ for some $q(x) \in R[x]$. Replace x by ω^j , we get

$$f(\omega^j) * g(\omega^j) = f(\omega^j)g(\omega^j) + 0.$$

$$\therefore DFT_\omega(f(x) * g(x)) = DFT_\omega(f(x)).DFT_\omega(g(x)).$$

Theorem 16 For a polynomial $f(x) \in R[x]$, $DFT_\omega^{-1}(f(x)) = \frac{1}{m}DFT_{\omega^{-1}}(f(x))$.

Proof 20 The matrix of the transformation $DFT_\omega(f(x))$ is

$$[DFT_\omega(f(x))] = \phi = \begin{pmatrix} 1 & 1 & 1 & \dots & 1 \\ 1 & \omega & \omega^2 & \dots & \omega^{m-1} \\ 1 & \omega^2 & (\omega^2)^2 & \dots & (\omega^2)^{m-1} \\ . & . & . & \dots & . \\ . & . & . & \dots & . \\ . & . & . & \dots & . \\ 1 & \omega^{m-1} & (\omega^{m-1})^2 & \dots & (\omega^{m-1})^{m-1} \end{pmatrix}$$

The matrix ϕ is the well known Vandermonde matrix and its inverse is $\frac{1}{m}\phi^*$, where ϕ^* is the matrix transpose conjugated [1]. Since ϕ is a square matrix and the conjugate of ω is ω^{-1} , we have $DFT_\omega^{-1}(f(x)) = \frac{1}{m}DFT_{\omega^{-1}}(f(x))$.

Example 4 We know that $R = Z_{49}$ is a halidon ring with index $m = 6$ and $\omega = 19$. Also, $\omega^{-1} = \omega^5 = 31$. Let $f(x) = 2 + x + 2x^2 + 3x^3 + 5x^4 + 10x^5 \in R[x]$. Then $DFT_\omega(f(x))$ can be expressed as

$$\begin{pmatrix} F_0 \\ F_1 \\ F_2 \\ F_3 \\ F_4 \\ F_5 \end{pmatrix} = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & \omega & \omega^2 & \omega^3 & \omega^4 & \omega^5 \\ 1 & \omega^2 & \omega^4 & 1 & \omega^2 & \omega^4 \\ 1 & \omega^3 & 1 & \omega^3 & 1 & \omega^3 \\ 1 & \omega^4 & \omega^2 & 1 & \omega^4 & \omega^2 \\ 1 & \omega^5 & \omega^4 & \omega^3 & \omega^2 & \omega \end{pmatrix} \begin{pmatrix} f_0 \\ f_1 \\ f_2 \\ f_3 \\ f_4 \\ f_5 \end{pmatrix} \Rightarrow \begin{pmatrix} F_0 \\ F_1 \\ F_2 \\ F_3 \\ F_4 \\ F_5 \end{pmatrix} = \begin{pmatrix} 23 \\ 24 \\ 32 \\ 44 \\ 9 \\ 27 \end{pmatrix}$$

$$\begin{aligned}
 \begin{pmatrix} f_0 \\ f_1 \\ f_2 \\ f_3 \\ f_4 \\ f_5 \end{pmatrix} &= 6^{-1} \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & \omega^5 & \omega^4 & \omega^3 & \omega^2 & \omega \\ 1 & \omega^4 & \omega^2 & 1 & \omega^4 & \omega^2 \\ 1 & \omega^3 & 1 & \omega^3 & 1 & \omega^3 \\ 1 & \omega^2 & \omega^4 & 1 & \omega^2 & \omega^4 \\ 1 & \omega & \omega^2 & \omega^3 & \omega^4 & \omega^5 \end{pmatrix} \begin{pmatrix} F_0 \\ F_1 \\ F_2 \\ F_3 \\ F_4 \\ F_5 \end{pmatrix} \\
 \Rightarrow \begin{pmatrix} f_0 \\ f_1 \\ f_2 \\ f_3 \\ f_4 \\ f_5 \end{pmatrix} &= 41 \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 31 & 30 & 48 & 18 & 19 \\ 1 & 30 & 18 & 1 & 30 & 18 \\ 1 & 48 & 1 & 48 & 1 & 48 \\ 1 & 18 & 30 & 1 & 18 & 30 \\ 1 & 19 & 18 & 48 & 30 & 31 \end{pmatrix} \begin{pmatrix} F_0 \\ F_1 \\ F_2 \\ F_3 \\ F_4 \\ F_5 \end{pmatrix} \\
 \text{If } \begin{pmatrix} F_0 \\ F_1 \\ F_2 \\ F_3 \\ F_4 \\ F_5 \end{pmatrix} &= \begin{pmatrix} 23 \\ 24 \\ 32 \\ 44 \\ 9 \\ 27 \end{pmatrix}, \text{ then a direct calculation gives } \begin{pmatrix} f_0 \\ f_1 \\ f_2 \\ f_3 \\ f_4 \\ f_5 \end{pmatrix} = \begin{pmatrix} 2 \\ 1 \\ 2 \\ 3 \\ 5 \\ 10 \end{pmatrix} \\
 &\text{as expected.}
 \end{aligned}$$

The programme-6 and programme-7 will enable us to calculate Discrete Fourier Transform and its inverse. We can cross-check the programmes against example 4.

$$\begin{aligned}
 \text{If } R = Z_{100001}, m = 10, \omega = 26364 \text{ and } f(x) = 1 + 2x + 3x^2 + 4x^3 + \\
 5x^4 + 6x^5 + 7x^6 + 8x^7 + 9x^8 + x^9 \in R[x], \text{ then } \begin{pmatrix} F_0 \\ F_1 \\ F_2 \\ F_3 \\ F_4 \\ F_5 \\ F_6 \\ F_7 \\ F_8 \\ F_9 \end{pmatrix} &= \begin{pmatrix} 46 \\ 19019 \\ 3314 \\ 10082 \\ 48017 \\ 4 \\ 80347 \\ 18172 \\ 68413 \\ 52627 \end{pmatrix}.
 \end{aligned}$$

Also, we can verify the inverse DFT using the above data.

8 Conclusions

The halidon rings are useful to extend the two famous theorems of Graham Higman(1940) and Maschke(1899). Since Higman's theorem and Maschke's theorem have a wide range of applications in group rings, group algebras and representation theory, there is a big scope of wider applications of halidon rings. The field of complex numbers is an infinite halidon ring with any index $m > 0$. The field of real numbers is an infinite halidon ring with index 2 and the ring integers is a trivial halidon ring with index $m=1$. Using the field of complex numbers, we can create infinite halidon rings of square matrices with any index $m > 0$. This will open new vistas of applications in algebra and number theory. Another area of application is the coding theory on which the author is currently working with.

Acknowledgment I am very much indebted to Prof. M.I.Jinnah, Former Head of Mathematics, University of Kerala, India, for his constructive suggestions and support.

References

- [1] P.J.Davis *Circulant Matrices* John Wiley & Sons, New York(1979).
- [2] Gordon James and Martin Liebeck *Representations and Characters of Groups* Cambridge University Press, New York (2001).
- [3] G. Higman *The Units of Group Rings* Proc. London Math. Soc. 46(1940), 231-248.
- [4] Joachim von zur Gathen and Jürgen Gerhard *Modern Computer Algebra, second edition* Cambridge University Press, Cambridge (2003).
- [5] G. Karpilovsky *Commutative Group Algebras* Marcel Dekker, No.78(1983).

- [6] Lang, Serge *Algebra* Graduate Texts in Mathematics, 211 (Revised 3rd ed.), New York: Springer-Verlag (2002).
- [7] N. Mohan Kumar and Pramod K. Sharma *A Graphical Representation of Rings via Automorphism Groups* <https://www.math.wustl.edu/kumar/papers/sharma.pdf>
- [8] K. N. Ponomaryov, *Automorphically rigid group algebras. I. Semisimple algebras* Algebra Logika, 48, No. 5, 654-674 (2009).
- [9] A. Telveenus *Circulants and Group Algebras* Hadronic Journal Supplement, Vol. 14, pp 227-288 (1999).
- [10] A. Telveenus *Halidon Rings and Group Algebras* Algebras, Groups and Geometries 18, pp 317-330 (2001).

9 Appendix

Programme-1 : To check whether $Z(n)$ is a trivial or nontrivial halidon ring

```
#include <iostream>
#include <cmath>
using namespace std;
int main() {
    cout << "To check whether Z(n) is a trivial or nontrivial halidon ring." << endl;
    unsigned long long int t = 0, n = 1, w = 1, hcf, hcf1,
    d = 1, k = 1, q = 1, p = 1, b=0, c=0, temp = 1;
    cout << "Enter an integer n >0: ";
    cin >> n;
    if (n % 2 == 0) {
        cout << "Z(" << n << ") is a trivial halidon ring." << endl;
    }
    for (w = 1; w < n; ++w) {
        for (int i = 1; i <= n; ++i) {
            if (w % i == 0 && n % i == 0) {
                hcf = i;
```

```
}
} if (hcf == 1) {
++t; // cout << " " << w << " ";
}
}
for (w = 1; w < n; ++w) {
for (int i = 1; i <= n; ++i) {
if (w % i == 0 && n % i == 0) {
hcf = i;

}
}
if (hcf == 1) {
for (int k = 1; k <= t; ++k) {
q = q * w; q = q % n;
if (q == 1) { if (temp <= k) { temp = k; } break; }
}
}
}

for (w = 2; w < n; ++w) {
for (int i = 1; i <= n; ++i) {
if (w % i == 0 && n % i == 0) {
hcf = i;
}
}
if (hcf == 1) {
for (int k = 1; k <= temp; ++k) {
q = q * w; q = q % n; if (q == 1) {
for (int i = 1; i <= n; ++i) {
if (k % i == 0 && n % i == 0) {
hcf1 = i;
}
}
}
if (hcf1 == 1) {
```

```
for (int j = 1; j < k; ++j)
{
    if (k%j == 0) {
        d = j;
        for (int l = 1; l <= d; ++l)
        {
            p = (p*w); p = p % n;
        }
        for (int i = 1; i <= n; ++i) {
            if ((p - 1) % i == 0 && n % i == 0) {
                hcf = i;
            }
        }

        if (hcf == 1) {

            p = 1; b = b + 1;
        }
        else p = 1;
        c = c + 1;
    }
}

if (c == b) { cout << "    Z(" << n << ")" <<

" is a halidon ring with index m= " << k <<

" and w= " << w << "." << endl; } {p = 1; c = 0; b = 0; }

break;
}
}
}
}
} return 0;
}
```

Programme-2: To check whether an element in Z_nG ; G is a cyclic group of order m has a multiplicative inverse or not

```
#include<iostream>
#include<cmath>
using namespace std;
int main() {
    cout << "To check whether an element in  $Z(n)G$ ;" <<
    "G is a cyclic group of order m" <<
        \has a multiplicative inverse or not" << endl;
    int a[100], b[100], c[100], d[100], e[100], w1[100], m = 1,
    t = 0, x = 1, s = 0, s1 = 0, l = 0, m1 = 1, hcf = 1,
    n = 1, i = 1, k = 0, q = 1, p = 1, r = 1, w = 1;
    cout << "Enter n =" << endl;
    cin >> n;
    cout << "Enter index m =" << endl;
    cin >> m;
    cout << "Enter  $m^{-1}$  =" << endl;
    cin >> m1;
    cout << "Enter primitive m th root w =" << endl;
    cin >> w;
    for (i = 0; i < m; ++i)
        { w1[i] = (long long int)pow(w, i)) % n;
    cout << "w1[" << i << "]" << w1[i] << endl; }
    for (int i = 1; i < m + 1; ++i) {
        cout << "Enter a["<<i<<"]=" << endl;
        cin >> a[i];
    }
    a[0] = a[m];
    for (int r = 1; r < m + 1; ++r) {
        for (int j = 1; j < m + 1; ++j)
        {
            l = (m - j + 2) % m;
            x = ((j - 1) * (r - 1)) % m;
            k = k + (a[l] * w1[x]) % n; k = k % n;
            // cout << "k=" << k << endl;
        }
    }
}
```

```
} c[r] = k; cout << "c[" << r << "]=" << c[r] << endl;
k = 0;
}
for (r = 1; r < m+1; ++r) {
for (int i = 1; i <= n; ++i) {
if (c[r] % i == 0 && n % i == 0) {
hcf = i;
}
}
if (hcf == 1) {
cout << "c[" << r << "] is a unit" << endl;
}
else { cout << "c[" << r <<
"] is a not unit. So there is no multiplicative inverse." <<
endl; t = 1; }
}
for (r = 1; r < m + 1; ++r) {
for (int i = 1; i <= n; ++i) {
e[r] = (c[r] * i) % n;
if (e[r] == 1) {
b[r] = i;
cout << " The inverse of c[" << r << "] is " << b[r] << endl;
}
}
}
b[0] = b[m];
for (int r = 1; r < m + 1; ++r) {
for (int j = 1; j < m + 1; ++j)
{
l = (m - j + 2) % m;
x = (m*m-(j - 1) * (r - 1)) % m; cout << "x= " << x << endl;
k = k + (m1*b[l] * w1[x]) % n; k = k % n;
cout << "k=" << k << endl;
}
}
d[r] = k; cout << "d[" << r << "]=" << d[r] << endl;
```

```
k = 0;
}
if (t == 1) {
    s = m;
mylabel2:
    cout << a[m - s + 1] << "g^(" << m - s << ") + ";
    s--;
    if (s > 0) goto mylabel2; cout <<
        "has no multiplicative inverse." << endl;
}
else {cout << "The inverse of ";
    s = m;
mylabel:
    cout << a[m - s + 1] << "g^(" << m - s << ") + ";
    s--;
    if (s > 0) goto mylabel; cout << "is" << endl;
    s1 = m;
mylabel1:
    cout << d[m - s1 + 1] << "g^(" << m - s1 << ") + ";
    s1--;
    if (s1 > 0) goto mylabel1; cout << "." << endl; }
return 0;
}
```

Programme-3: To find idempotents, involutions and units in Z_n

```
#include<iostream>
#include<cmath>
using namespace std;
int main() {
    cout << "To find idempotents, involutions and units in  $Z(n)$ ." << endl;
    long long int i, j=0, n, k=0, x, y;
    cout << "Enter n=" << endl;
    cin >> n;
    cout << "The involutions are ";
    for (i = 1; i < n + 1; ++i) {
```



```
x = (i * i) % n;
if (x == 1) { cout << i << " "; }
} cout << "." << endl;
cout << "The idempotents are ";
for (i = 0; i < n + 1; ++i) {
x = (i * i) % n;
if (x == i) { cout << i << " "; j++; }
} cout << "." << endl; cout <<
    "Number of idempotents = " << j << endl;
cout << "The units and its inverse are " << endl;
for (y = 1; y < n + 1; ++y) {
for (i = 1; i < n + 1; ++i) {
x = (y * i) % n;
    if (x == 1) { cout << y << " , " << i << endl; k++; }
}
} cout << "Number of units = " << k;
return 0;
}
```

Programme-4: To find the inverse of an element in $Z(n)G$; G is a cyclic group of order m through λ units

```
#include<iostream>
#include<cmath>
using namespace std;
int main() {
cout << "To find the inverse of an element in  $Z(n)G$ ;" <<
"G is a cyclic group of order  $m$  through  $\lambda$  units." << endl;
int a[100], b[100], l[100], li[100], w1[100],
m = 1, t = 0, x = 1, y=1, s = 0, si = 0, m1 = 1, hcf = 1, n = 1,
i = 1, k = 0, q = 1, p = 1, r = 1, w = 1;
cout << "Enter n =" << endl;
cin >> n;
cout << "Enter index m =" << endl;
cin >> m;
```

```
cout << "Enter m^(-1) =" << endl;
cin >> m1;
cout << "Enter primitive m th root w =" << endl;
cin >> w;
for (i = 0; i < m; ++i) { w1[i] = ((long long int)pow(w, i)) % n;
cout << "w1[" << i << "]= " << w1[i] << endl; }
cout << "Enter lamda values which have inverse" << endl;
for (int i = 1; i < m + 1; ++i) {
cout<< "l[" << i << "]= " << endl;
cin >> l[i];
}
cout << "Enter lamda inverse values " << endl;
for (int i = 1; i < m + 1; ++i) {
cout << "l1[" << i << "]= " << endl;
cin >> l1[i];
}
for (int r = 1; r < m + 1; ++r) {
for (int j = 1; j < m + 1; ++j)
{
x = ((j - 1) * (r - 1)) % m;
k = k + (m1*l[j] * w1[x]) % n; k = k % n;
// cout << "k=" << k << endl;
} a[r] = k; cout << "a[" << r << "]= " << a[r] << endl;
k = 0;
}
for (int r = 1; r < m + 1; ++r) {
for (int j = 1; j < m + 1; ++j)
{
x = ((j - 1) * (r - 1)) % m; cout << "x= " << x << endl;
k = k + (m1 * l1[j] * w1[x]) % n; k = k % n;
cout << "k=" << k << endl;
} b[r] = k; cout << "b[" << r << "]= " << b[r] << endl;

k = 0;
}
```

```
cout << "The inverse of a= ";
s = 1;
mylabel:
cout << a[s ] << "g^(" << s-1 << ") + ";
s++;
if (s < m+1) goto mylabel; cout << endl;  cout << "is b=";
s1 = m;
mylabel1:
cout << b[m - s1 + 1] << "g^(" << m - s1 << ") + ";
s1--;
if (s1 > 0) goto mylabel1; cout << "." << endl;
cout << "Note: Please neglect the last + as" <<
      "it is unavoidable for a for loop.";
return 0;
}
```

Programme-5: To find the idempotent elements in Z_nG ; G is a cyclic group of order λ takes idempotent values in Z_n

```
\begin{verbatim}
#include<iostream>
#include<cmath>
using namespace std;
int main() {
cout << "To find the idempotent elements in  $Z(n)G$ ;"<<
"G is a cyclic group of order m through" <<
"lambda takes idempotent values in  $Z(n)$ ." << endl;
int a[100], l[100], w1[100], m = 1, t = 0, x = 1, y = 1, s = 0,
s1 = 0, m1 = 1, n = 1, i = 1, k = 0, r = 1, w = 1;

cout << "Enter n =" << endl;
cin >> n;
cout << "Enter index m =" << endl;
cin >> m;
cout << "Enter  $m^{(-1)}$  =" << endl;
cin >> m1;
```

```
cout << "Enter primitive m th root w =" << endl;
cin >> w;
for (i = 0; i < m; ++i) { w1[i] = ((long long int)pow(w, i)) % n;
cout << "w1[" << i << "]=" << w1[i] << endl; }
cout << "Enter lamda values which are idempotents" << endl;
for (int i = 1; i < m + 1; ++i) {
cout << "l[" << i << "]=" << endl;
cin >> l[i];
}
for (int r = 1; r < m + 1; ++r) {
for (int j = 1; j < m + 1; ++j)
{
x = ((j - 1) * (r - 1)) % m;
k = k + (m1 * l[j] * w1[x]) % n; k = k % n;
}
a[r] = k; cout << "a[" << r << "]=" << a[r] << endl;
k = 0;
}
cout << "The idempotent element in RG is e= ";
s = 1;
mylabel:
cout << a[s] << "g^(" << s - 1 << ") + ";
s++;
if (s < m + 1) goto mylabel; cout << endl;
cout << endl;
cout << "Note: Please neglect the last + as it is" <<
"unavoidable for a for loop.";
return 0;
}
```

Programme-6: Discrete Fourier Transform

```
#include <iostream>
#include<cmath>
using namespace std;
```

```
int main()
{
    cout << "Discrete Fourier Transform" << endl;
    unsigned long long int a[200][200], b[200][200],
    mult[200][200], q=1, m=1, n=1, w2=1, w=1, r1, c1, r2,
    c2, i, j, k, t=1;
    cout << "Enter n,m,w: ";
    cin >> n >> m >> w;
    r1 = m; c1=m;
    r2 = m; c2=1;
    for (i = 0; i < r1; ++i)
    for (j = 0; j < c1; ++j)
    {
        t = (i*j)%m;
        if (t == 0) a[i][j] = 1;
        else
        for (q = 1; q < t + 1; ++q) { w2 = (w2 * w) % n; }
        a[i][j] = w2; w2 = 1;
    }
    for (i = 0; i < r1; ++i)
    for (j = 0; j < c1; ++j)
    {
        cout<<" a"<<i+1<<" "<<j+1<<"="<<a[i][j] ;
        if (j == c1 - 1)
        cout << endl;
    }
    cout << endl << "Enter coefficient vector of
    the polynomial:" << endl;
    for (i = 0; i < r2; ++i)
    for (j = 0; j < c2; ++j)
    {
        cout << "Enter element f" << i << " = ";
        cin >> b[i][j];
    }
    for (i = 0; i < r1; ++i)
```

```
for (j = 0; j < c2; ++j)
{
    mult[i][j] = 0;
}
for (i = 0; i < r1; ++i)
for (j = 0; j < c2; ++j)
for (k = 0; k < c1; ++k)
{
    mult[i][j] += (a[i][k]) * (b[k][j]);
}
cout << endl << "DFT Output: " << endl;
for (i = 0; i < r1; ++i)
for (j = 0; j < c2; ++j)
{
    cout << "F"<< i << "="<< mult[i][j]%n;
    if (j == c2 - 1)
        cout << endl;
}
return 0;
}
```

Programme-7: Inverse Discrete Fourier Transform

```
#include <iostream>
#include<cmath>
using namespace std;
int main()
{
    cout << "Inverse Discrete Fourier Transform" << endl;
    unsigned long long int a[100][100], b[100][100],
        mult[100][100], p=1, q=1, l=1, m = 1, m1 = 1, w1 = 1,
        w2=1, n = 1, w = 1, r1, c1, r2, c2, i, j, k,
        c=1,t = 1;
    cout << "Enter n,m, w: ";
    cin >> n >> m >> w;
```

```
for (l = 1; l < n; ++l)
{
    c = (l * m) % n;
    if (c == 1)
    {
        m1 = l;
    }
}
for (p = 1; p < m; ++p)
{
    w1 = (w1 * w) % n;
}
r1 = m; c1 = m;
r2 = m; c2 = 1;
for (i = 0; i < r1; ++i)
for (j = 0; j < c1; ++j)
{
    t = (i * j) % m;
    if (t == 0) a[i][j] = 1;
    else
    for (q = 1; q < t + 1; ++q) { w2 = (w2 * w1) % n; }
    a[i][j] = w2; w2 = 1;
}
for (i = 0; i < r1; ++i)
for (j = 0; j < c1; ++j)
{
    cout << "  a" << i + 1 << j + 1 << "=" << a[i][j];
    if (j == c1 - 1)
    cout << endl;
}
cout << endl << "Enter DFT vector :" << endl;
for (i = 0; i < r2; ++i)
for (j = 0; j < c2; ++j)
{
    cout << "Enter element F" << i << " = ";
}
```

```
cin >> b[i][j];
}
for (i = 0; i < r1; ++i)
for (j = 0; j < c2; ++j)
{
mult[i][j] = 0;
}
for (i = 0; i < r1; ++i)
for (j = 0; j < c2; ++j)
for (k = 0; k < c1; ++k)
{
mult[i][j] += (a[i][k]) * (m1 * b[k][j]);
}
cout << endl << "Polynomial vector: " << endl;
for (i = 0; i < r1; ++i)
for (j = 0; j < c2; ++j)
{
cout << "f" << i << "=" << mult[i][j] % n;
if (j == c2 - 1)
cout << endl;
}
return 0;
}
```


**ADVANCING COMPUTATIONAL SPACE VALUE THEORY [CSVT]
FOR MULTIVALENT GAME MECHANICS**

Jonah Lissner

Canadian Journal of Pure and Applied Sciences
Computational Intelligence Group, University of Manitoba
editor@cjpas.org

Received March 10, 2021

Revised October 6, 2021

Abstract

For the purpose of decision structure mechanics of computational engineering, a bivalent unlimited, or cardinal infinite computational algorithm space quantum game is estimated in multivalent algorithm and quantum group mechanics.

Keywords: Computational Value Space Theory [CSVT], Quantum Game Theory, Quantum Bayesian, Multivalent Logic, Banach-Mazur Game

1 Introduction

When estimating for a bivalent unlimited, or cardinal infinite computational algorithm space quantum game, multivalent algorithm and quantum group mechanics can be demonstrated.

This question can utilize multivalent algorithm theory[1] and quantum group variation of the quantum computational Zeno paradox given a Quantum Neural Network [QNN] or Quantum Finite State Machine [qFSM], where generally

$$Pr(\sigma) = \| PU_{\sigma_k} \cdots U_{\sigma_1} U_{\sigma_0} |\psi\rangle \|^2 \quad (1)$$

from the string

$$\sigma = (\sigma_0, \sigma_1, \dots, \sigma_k). \quad (2)$$

in a Hopfield Network where

$$J_{pseudo-cut}(k) = \sum_{i \in C_1(k)} \sum_{j \in C_2(k)} w_{ij} + \sum_{j \in C_1(k)} \theta_j. \quad (3)$$

Given a bivalent [monoidal] decision grid for a word problem such that

$$S_w = \langle X | R \cup \{w\} \rangle, \quad (4)$$

or group word problems as interpretation sets forming a general species of game Semantics. In a Universe of Discourse and objects $\mathbf{jM}(\phi)$,

Let

$$\mathbf{D} :: E(x, y) = \{ \epsilon_i(x, y) : i \in I \}, \quad (5)$$

where

$$\Gamma \approx \Delta \models_K \varphi \approx \psi \text{ iff } E(\Gamma, \Delta) \vdash_D E(\varphi, \psi), \quad (6)$$

[Encyclopedia of Mathematics]

This can be demonstrated in Dyadic theory, whence opponents **A** and **B** of an algorithm game the value of their own logic, versus their opponent's algorithm, generating isomorphisms of Shared Value, [Monoidal, Symmetrical Strategy, Idealistic] or Singular Value, [Isomorphic, Asymmetric Strategy, Pragmatic] in methods like reversible cellular automata.

Methods and Mechanics

In the inherent practical and Infinitary multivalent logic Computational Space Value Theory [CSVT] of the nonlinear system, mechanics and probability boxes can be demonstrated where in general formula for

"**P** **R**, i.e., $\mathbb{D} = \{D \mid D : \mathbb{R} \rightarrow [0,1], D(x) \leq D(y) \text{ whenever } x < y, \text{ for all } x, y \in \mathbb{R}\}$, and let **I** denote the set of real intervals, i.e., $\mathbb{I} = \{i \mid i = [i_1, i_2], i_1 \leq i_2, i_1, i_2 \in \mathbb{R}\}$. Then a **p**-box is a quintuple $\{F, \underline{F}, m, v, F\}$, where $F, \underline{F} \in \mathbb{D}$, while $m, v \in \mathbb{I}$, and $F \subseteq \mathbb{D}$." (7)

[*ibid*]

In Helly metric this word problem matrix can be proposed in the general formula

$$\rho(x_1, x_2) = \sup_{y \in \mathcal{Y}} |H(x_1, y) - H(x_2, y)|, \quad (8)$$

and

$$\rho(y_1, y_2) = \sup_{x \in \mathcal{X}} |H(x, y_1) - H(x, y_2)|, \quad (9)$$

where $H = H$ is equivalent to ENDGAME.

It is proposed a 3+1D >> 2^4=16 value assessment in a game scenario of **A** versus **B** and imaginary values and computational game decision variables by utilizing potential ideal Thesis and ideal Data of informational sets, from

probability of values and objects in the real intervals derived from potential ideal Value.

Relativity of value is therefore metricized for actual value evaluation from value criteria of ideal data, and subsequent utilization for a prospective topological power theory of networks, Blum-Shub-Smale Machine [BSS] machines, Zipf's Law, Restricted Boltzmann Machines, and types of quantum cellular automata mechanics for given set arrays of probability functions.

The Bayesian equation

$$d(X, Y) = H(X, Y) - I(X; Y) = H(X) + H(Y) - 2I(X; Y) = H(X|Y) + H(Y|X) \quad (10)$$

can be used for information entropy distribution and as a function where

$$I(X; Y) = \int_Y \int_X p(x, y) \log \left(\frac{p(x, y)}{p(x)p(y)} \right) dx dy, \quad (11)$$

Regarding game situational rules, no real pragmatical purpose for defeat is offered for pragmatic value theory, and a situation of total rhetorical war ensues to the detriment of real Ideal value. As in a multiple-game scenario of a Mermin-Peres square given

$$|\phi\rangle = \frac{1}{\sqrt{2}} \left(|+\rangle_a \otimes |+\rangle_b + |-\rangle_a \otimes |-\rangle_b \right) \otimes \frac{1}{\sqrt{2}} \left(|+\rangle_c \otimes |+\rangle_d + |-\rangle_c \otimes |-\rangle_d \right) \quad (12)$$

where

$$S_x = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, S_y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}, S_z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

(13)

algebraic structure of the spin cube or possible spin jam, both A and B have a degree of probability if neither plays to win, to a earn either a stalemate as in Chess Theory, or a win for either A or B.

A methodology of 2D automata choice in an estimation of the Computational Space Value Theory [CSVT] is predicted to be mostly loss-based if used in a pure quantum setting for 4 cell variables per turn or 0 or 1 quantum cell variables per turn, and increasingly win-based with 3 quantum cell variables per turn or 2 quantum cell variables per turn versus a purely classical automata, and increasingly prone to complete tie or agreement in strategy and generations being versus an evenly-matched other quantum automata.

A 1-cell degree of quantum automata of 0 through 4 is decided to a greater dimensional requirement that a 2-dimensional automata board can generate in the Computational Space Value Theory [CSVT] classical and quantum game, and may be decided in quantum logic terms or multivalent logic terms cell-by-cell, and additionally by degrees of alternative altruism variables in degrees or variations of this previous sequence. [2]

An answer may be found from Booth[3] which demonstrates Qualitative and Practical Computational Space Value Theory [CSVT] modes which ultimately can be engineered as tools for algorithm theory and Decision mapping[4] in 2D and 3D cellular automata games and evolutionary mapping.

This game is similar to 2D or 3D Go game theory, evolutionary landscape projections and algorithmic information mechanics of Minimum Message Length where E has probability

$$P(E) \text{ where } (E) = -\log_2(P(E)) \quad (14)$$

and to Solomonoff evolutionary inductive computing machines and can be advanced in the mathematical structure.

2 Theorems and Results

In a Computational Space Value Theory [CSVT] matrix for the dialectic regarding Game Theory of Booth's rhetoric, game, competition, computation and cooperation, Practical or Pragmatists [A] argue that the given qualitative game Objective Value, and Game Ideal has arelevance and weight the Game value language thusly; Intellectual or Idealists [B] argue that the practical resolution relevance is only transitory to the Game Ideal and so weight the game ideal.

Given Quine's New Riddle of Induction [Blue blue/breen : gleen/green Green], in which space can the two compete in game competition, or avoid problems of inductive inference or Hempel's paradox, and What is the Expected Utility Hypothesis for each camp?

Carnap proposed for probability equations

$$P(Fa|E) = \frac{n_F + \lambda P(Fa)}{n + \lambda} \quad (15)$$

and in the Bayesian approach the formula

$$\text{bel}(A) + \text{bel}(\bar{A}) = 1 \text{ for all } A \subseteq X. \quad (16)$$

A simple Long-Short-Term Memory Recurrent Neural Network [LSTM-RNN][5] can be constructed with gradient descent and backpropagation to learn-evolve words, multiple evolutionary word clusters and strings and Long-Short-Term Memory [LSTM] blocks into computable word-sheafs and books utilizing Rhetorical Structure Theory [RST] and evolutionary Hash Tables:

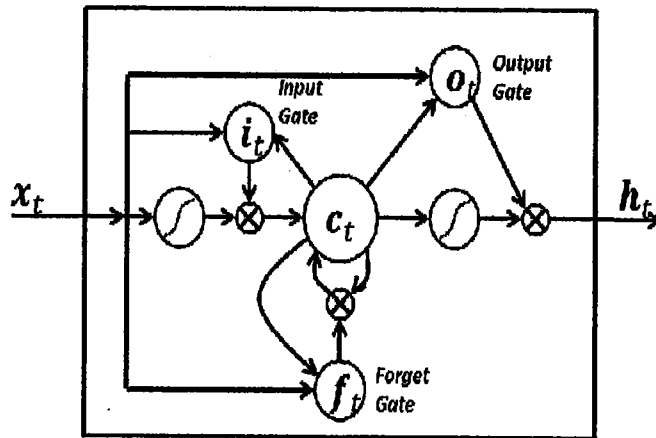


Fig. 1: "Long short-term memory: A simple LSTM block with only input, output, and forget gates", extracted, Wikimedia.

Input [On-And], Output [Off-Not], Forget>>On-Off [XOR] As Finite state-machines [FSM] or quasi-FSM [qFSM] modules, these are the basis for the algorithm decision first line of game moves, and have one-unit initial value, with the exception of pas de deux or in altruistic gambles in Chess, given for the Algorithm Sheaf, and in Quantum Automata-based Programming.

According to Von Neumann-Morgenstern in this game decision $A \succeq B$ or $A \preceq B$, the example of Zero-determinant strategies [Press, Dyson] and the Rule of Diminishing Return or Ultimatum, is a method based on scalar variables in algorithm landscape, to reduce game differences and resources between any two ideological opponents, like Donation Game [Stewart, Plotkin] unless a Pragmatic or Ideal approach to the game Objective Value is viable, in Domination, Incremented-Determination, or Fusion Strategy.

In the matter of game cooperation or strategic assent, or conversely game strategic dissent, the proper action may be on the Matrix $\mathbf{M} \langle \mathbf{A}, \mathbf{B} \rangle$ which is the ordinal set of the matrix for all imaginary P1, P2, I1, I2 Algorithm ranges for A and "... Algorithm ranges for N with intermediary or local zeta functions.

Iterated Function System [IFS] mechanics can be proposed where for $F: S \rightarrow S$ and $F^{(n)} = F \circ F \circ \dots \circ F$, (17)

then $O_F(P) = \{P, F(P), F^{(2)}(P), F^{(3)}(P), \dots\}$. (18)

Per Uniform Boundedness Conjecture [UBC, Morton and Silverman] it can be stated

$F: \mathbf{PN} \rightarrow \mathbf{PN}$ for $\mathbf{PN}(K)$. (19)

Game cooperation in resource competition is not so simple. How is Booth's version of the Narrator applying the perceived ideal Value utilized in the proposed quantum set logic states? In Booth's dialectic the Intellectual, Qualitative and Practical modes have been applied. The veracity or accuracy of the rulebase is the focus by which a game algorithm exists. Booth proposes the existence of Rules as indexes by which the Reader must be critical of the

Narrator. However in the review of the opposing side, indexes of Algorithms and Decisions are also mutable and subject to Decision algorithm structure.

An answer is proposed here in the quality and value for given potential ideal Value for the ideal Value, the derived ideal Thesis, from which A and B utilize their decisions. By the admittance of the ideal Thesis, the Opposing Agents can reinvest practical and ultimately ideal value, to the value space of the rhetorical spaces.

By the usage of the ideal Thesis, the Qualitative, Realistic or Practical are seen as elements of the same Quality of Algorithm in the quantum probability field in Multivalent matrices. The value of the word-algorithm is proposed to have potential value in the pragmatic application by the Narrator in the Regime to discover its Ideal and Practical potential or implied and practiced or applied value.

3 Lemma

If Qualitative algorithm demands x for y from A, and B demands x1 for y1, the Practical mode of Bivalence is invoked; what is the real and perceived cost for x1 for y1 or y for x, for either party, and how can they be decided?

Common ground of the information physics for the Computational Space Value Theory [CSVT] is proposed in the computed value space for degrees of Truth and subsequent truth tables in 2D for bivalent approaches and Karnaugh maps and topologies in 3D for multivalent approaches. Cheon and Tsutsui have advanced classical evolutionary game theory and quantum game theory on the Hilbert space[6] where

$$|\alpha, \beta; \gamma\rangle = J(\gamma) |\alpha\rangle_A |\beta\rangle_B, (1) \text{ and } \Pi_A(\alpha, \beta; \gamma) = \langle \alpha, \beta; \gamma | A | \alpha, \beta; \gamma \rangle, (2) \Pi_B(\alpha, \beta; \gamma) = \langle \alpha, \beta; \gamma | B | \alpha, \beta; \gamma \rangle \quad (20)$$

for various phases of quantum Nash equilibrium payoff and Quantal response equilibrium.

It is here that the potential probability of agreement is reached by the Opposing Agents if they must acknowledge the other's Ideal Thesis [That if X is so, therefore] for the Cardinality of the given continuum of infinitary Space Value of computation to exist. This coexistent multivalent set measure continuum

phenomenon of potential ideal Value, communicates in methods of computational-mode thermodynamics.

It can further be gauged by Vapnik-Chervonenkis Theory of statistical learning in rate of convergence of learning and consistency of gaugability of the given infinitary Space Value of computation gaming topology.

The Vapnik-Chervonenkis dimension demonstrates algorithmic thresholds and cardinals of epistemological meaning in general Let

$$\begin{aligned}
 &X_1, X_2, \dots, X_n \text{ for } (\mathcal{X}, \mathcal{A}) \\
 &\mathbb{P}_n = n^{-1} \sum_{i=1}^n \delta_{X_i}, \\
 &\text{then} \\
 &\text{and } Qf = \int f dQ.
 \end{aligned} \tag{21}$$

4 Proof

From the potential ideal thesis generates the potential implied Author of Booth, the author of the ideal data. Therefore construction of Rhetoric as grounding empirical hypothesis, and assorted rules, are therefore supposed to generate less statistical relevance. It is hypothesized that without the acknowledgement of the antithesis in the other's ideal Thesis for the solution of ideal Data:

[If X, then Y is equivalent in the Game Matrix, therefore the Exhibit Z must demonstrate radicals of calculated differentials or equivalence in $M\langle A, B \rangle$].

Expected game utility of this algorithm is in general

$$\begin{aligned}
 E[u(w)] &= E[w] - b E[e^{-aw}] \\
 &= E[w] - b E[e^{-a E[w] - a(w - E[w])}] \\
 &= E[w] - b e^{-a E[w]} E[e^{-a(w - E[w])}] \\
 &= \text{Expected wealth} - b \cdot e^{-a \cdot \text{Expected wealth}} \cdot \text{Risk}.
 \end{aligned} \tag{22}$$

The ideal data Mapping for all **P1, P2, I1, I2, N + log₂N** Algorithm ranges of **M<A,B>** generates the theoretical structure for the First Mode of Value Space in Game Theory Value for proofs.

Therefore the baseline Unreliability [Quantum Uncertainty] of the Narrative can at least be assumed from analysis to have enough *potential value* for the purpose of the result, if this probability parsing of Computational Space Value Theory [CSVT] is utilized to practical application in idea and in algorithm for Quantum Bayesian Networks where generally

$$P(G, S, R) = P(G|S, R)P(S|R)P(R). \quad (23)$$

This can be based on a conditional probability where

$$P(S/T) = P(S \& T)/P(T) \text{ and } P_f(S) = P_i(S/E). \quad (24)$$

Random decision matrix variables can be formulated in Bayesian method where

$$P(R = T | G = T) = \frac{P(G = T, R = T)}{P(G = T)} = \frac{\sum_{S \in \{T, F\}} P(G = T, S, R = T)}{\sum_{S, R \in \{T, F\}} P(G = T, S, R)}. \quad (25)$$

Furthermore recurring common or cumulative grammatical variables can be parsed

$$\forall X \subseteq U_p[CUM_p(X) \Leftrightarrow \exists x, y[X(x) \wedge X(y) \wedge \neg(x = y)] \wedge \forall x, y[X(x) \wedge X(y) \Rightarrow X(x \oplus y)]] \quad (25)$$

where **Xset {T,F}** at statements from $\emptyset^{(n)}$.

Milner's Calculus of Communicating Systems added

$$P ::= \emptyset \mid a.P_1 \mid A \mid P_1 + P_2 \mid P_1|P_2 \mid P_1[b/a] \mid P_1 \backslash a. \quad (26)$$

For algorithmic computation each synchronized primitive value and set is treated as a history monoid of the generic product

$$P(A) = \Sigma_1^* \times \Sigma_2^* \times \cdots \times \Sigma_n^*. \quad (27)$$

An estimation of a 50.000_1% victory in a multivalent 2D algorithm graphing in an Ab v B. game space can be demonstrated where for

$$(Z/2Z^n) \text{ such that } Z^2 \text{ and } p_c = 1/2 \text{ at approximately } p_c = 1/(z - 1): \quad (28)$$

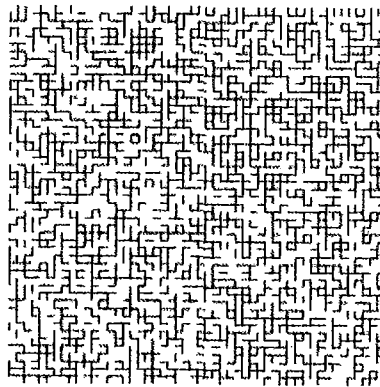


Fig. 2: "Algorithm Theory: Detail of a bond algorithm on the square lattice in two dimensions with algorithm probability $p = 0.51$ ", article, Wikimedia
In a number addition or computational matrix, the algorithm computability can furthermore be distributed at approximately [in Multivalent Logic] 100% of the CFD.

5 Section Summary

Computational Space Value Theory [CSVT] and infinitary space value models have been demonstrated for potential and ideal Thesis to potential and ideal Data in potential ideal Value, for Applied Monadic Mathematics-Information Natural Dynamics [AMM-IND] to quantum algorithms and game theory.

As opposed to 1st Mode of ideal definition, in actual definition the value of potential ideal Data is the 2nd Mode of Value Space, and the 3rd Mode of Computational Space Value Theory [CSVT] is the ideal usable data for any 4th Mode Decision from the Algorithm Mapping series.

The analysis must be weighed from potential application of points of data in the 4D game space topology. In the Bridging of $X \leftrightarrow Y$ these facts can be

estimated if True for the purposes of the potential ideal thesis they are useful and aggregated and weighted. If False these facts can be estimated for the purposes of the potential ideal thesis they are not useful and discarded.

These quantum mechanics are specifically derived from dissipative quantum Information Natural Dynamics [IND] Type Values for Applied Monadic Mathematics [AMM]:

Natural Sets, Natural Kinds, Natural Procedures, Natural Strings, Natural Radicals, Natural Binaries, Natural Radix; p-adic quantum automata; Granular Dynamics.

From Information Natural Dynamics [IND] Formula Values:

Time-Complexity, Particle-Value, Particle-Weighting in Multivalent set theory, Gravity of System, $\langle\langle\rangle\rangle$ Topodynamics of System variables [TC-PV-PW-GS-NDS].

6 Mathematical Ansatz

This lemma is demonstrated in greater logical and topological computational complexity on the Morse Topos for

$$f: M \rightarrow \mathbf{R} \text{ on } M^a = f^{-1}(-\infty, a] \quad (29)$$

such as in Traced Monoidal Categories where

$$\text{Tr}UX, Y: C(X \times U, Y \times U) \gg C(X, Y) \text{ so naturally } f(g) = f(g \times U).$$

(30)

Generally a Morse inequality on a 2-Manifold can be demonstrated modularly where

$$C^\gamma - C^{\gamma-1} \pm \cdots + (-1)^\gamma C^0 \geq b_\gamma(M) - b_{\gamma-1}(M) \pm \cdots + (-1)^\gamma b_0(M). \quad (31)$$

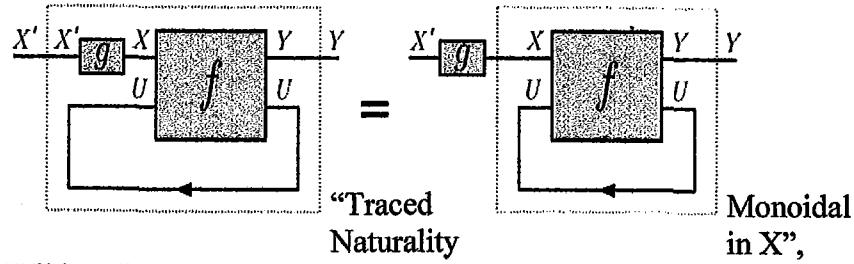


Fig. 3:
Category:
extracted, Wikimedia

Holomorphically the Morse Lemma can be utilized for the given computational word structure or monadic automata, as a Monadic Instruction Set Computer from the memristor formula, which can be demonstrated approximately

$$E_{\text{switch}} = V^2 \int_{T_{\text{off}}}^{T_{\text{on}}} \frac{dt}{M(q(t))} = V^2 \int_{Q_{\text{off}}}^{Q_{\text{on}}} \frac{dq}{I(q)M(q)} = V^2 \int_{Q_{\text{off}}}^{Q_{\text{on}}} \frac{dq}{V(q)} = V \Delta Q \quad (32)$$

where the Morse lemma descent for the combinatoric word structure is demonstrated

$$f(x) = f(b) - x_1^2 - \cdots - x_\alpha^2 + x_{\alpha+1}^2 + \cdots + x_n^2 \quad (33)$$

at a 1-cell interval from

$$\{[n, n+1]: n \in \mathbb{Z}\} \text{ on the } \mathbb{R}^n \quad (34)$$

for a computational synapse. This advances the Morse-Thue sequence and further Combinatoric sets of words and grammar on the topos-sheaves.

7 Defining Universal Computation Axioms with Information Entropy Variables

To specify filtering information density collapse within NP-hard, non-NP-complete delimits, a universal quantum Hamiltonian is proposed useful in the Universal Oracle Machine hypothesis. A Universal Computation Machine [UCM] is utilized for universal quantum computation in qualia of information entropy maximals where in general formula for the distributions

$$p_i = \frac{1}{n} \text{ for all } i \in \{1, \dots, n\}; \quad (35)$$

or Universal Quantum Probability Computing Machines [UQPCM], in a simplex basis for differential geometric number spaces in

$$q(t) \in Q \text{ via } |\Psi(q,t)|^2 \quad (36)$$

for a theoretical methodology for incomputables.
Shannon computed

$$H_c = - \int p(x) \log \frac{p(x)}{m(x)} dx \quad (37)$$

for the principle of continuous maximum information entropy algebraic information structures. It is unknown how sufficiently quantum, a theory definition of causal topology is required for a geometrization solution for the Poincare conjecture, utilizing a nonlinear system to measure Ricci condensation for continuous minimum information entropy algebraic information structures.

In quantum mechanics a k-local Hamiltonian can be computed for Quantum Merlin Arthur [QMA] completeness. It is conjectured to explain configuration of the energy landscape, without which the Universal Quantum Probability Computing Machines [UQPCM] is incomplete. Here

$$\bar{h}(a, x) \mapsto \bar{h}'(a, x) = \bar{h}(f^{-1}(a), f(x)), \quad (38)$$

and

$$S = \int \left[\frac{1}{2\kappa} (\mathcal{R} - 2\Lambda) + \mathcal{L}_M \right] (\det h)^{-1} d^4x. \quad (39)$$

Regarding the relativistic particle condensation on strings[7] for thermo-entropic chirality and quantum ergodics De Broglie-Bohm-Hiley-Bekenstein Holographic Principle [DBBHBHP] advances the similarities between dissipative and nonlinear systems, as essentially quantum information machine models. This advances a stronger algorithm against the reductionist hypothesis, reducing the hypothesis for purported solutions to Physical constants to program-run statements for generic classes of Universal Computational Machines [UCM].

Freund hypothesizes:

In the usual Archimedean bosonic string, when N D-branes coincide, a $U(N)$ symmetry with the attendant Chan-Paton (CP) rules is known to emerge. Does something similar happen in the p -adic case as well? A possible theory of p -adic strings with CP rules has been proposed [6]. It had the undesirable feature that for $N = 1$ its amplitudes did not reduce to the those of the theory without CP rules described above. This problem can be corrected by constructing an alternative p -adic string with CP rules as follows. In the lagrangian (4) let ϕ denote not a unique real scalar field, but an $N \times N$ matrix of such fields, with L_p obtained from Eq. (4) by taking the matrix trace. Then the theory clearly reduces to what it should for $N = 1$. The question that remains to be answered is: what is the worldsheet description of the p -adic theory whose effective tachyon action is given by this matrix-alternative construction? [*ibid*]

8 Discussion

Supplementary to this question is Quantum Entanglement and its relation to Quantum Computational Physics. Schrodingerian heuristics of quality and quantum of information states from Heisenberg and Planck units, interface in the two-state computation process. As a Universal self-organizing phenomena

of a given two-state thermodynamic process group the algebra is represented in a Clifford quadratic where

$$Cl(v, Q) \text{ and where } z_{n+1} = z_n^2. \quad (40)$$

Furthermore, the quantum computation is proposed to originate from n Time-sources in $\mathbf{R}^4$ for computability space across a propagative space. In engineering utilization the collective-distributed swarm computation can be applied to a Dyson formula where

$$a = \sqrt[3]{\mu \left(\frac{P}{2\pi} \right)^2}. \quad (41)$$

These algorithms are proposed in computation formula

$$S \mathbf{x}_i \in \mathbf{R}^n \text{ where } f(a) < f(b) \quad (42)$$

for value operations across complex network vector locations. Machine-based swarm intelligence can be utilized in other theory and mechanics of network theory and artificial intelligence:

In the q-calculus where

$$q = e^{ih} = e^{2\pi i \hbar} \quad (43)$$

demonstrates contemporaneous of quantum cellular oppositions for n -ary grain relations in a quantum complex network where atomically

$$|\psi_{ij}\rangle = |\phi\rangle_i \otimes |\phi\rangle_j, \quad (44)$$

for global optimization solutions and not maximal entanglement. This can be advanced with finitary operations of Universal algebra clone sets on lattices.

Therefore it can be stated relativistic n -ary relations of an existing computational state in entropic time are conjectured as Infinite in Chaitin's constant where

$$\Omega_F = \sum_{p \in P_F} 2^{-|p|}, \quad (45)$$

defined in polylogarithmic timescales, and in Planck time where

$$t_P \equiv \sqrt{\frac{\hbar G}{c^5}} \approx 5.39106(32) \times 10^{-44} \text{ s} \quad (46)$$

These are proposed to advance any+all Time complexity **#P** states for polynomial computations simultaneously generally = to **BQP** in **PSPACE**-completion or in quantum differential calculus where

$$d : A \rightarrow \Omega^1 \text{ and } d(ab) = a(db) + (da)b, \forall a, b \in A. \quad (47)$$

Here q-analog on a Fuchsian group in function $q \rightarrow 1$ where

$$\lim_{q \rightarrow 1} \frac{1 - q^n}{1 - q} = n \quad (48)$$

and where n is the modulo for the differential calculus.

Landau-Zener models demonstrate two-state and additionally or multi-state perturbation regime in thermodynamic quantum mechanics and regimes[8],

$$P_D = e^{-2\pi\Gamma}$$

$$\begin{aligned} \Gamma &= \frac{a^2/\hbar}{\left| \frac{\partial}{\partial t}(E_2 - E_1) \right|} = \frac{a^2/\hbar}{\left| \frac{dq}{dt} \frac{\partial}{\partial q}(E_2 - E_1) \right|} \\ &= \frac{a^2}{\hbar |\alpha|} \end{aligned}$$

$$\text{where} \quad (49)$$

Shor's Algorithm proposes quantum phase estimation algorithmic formulas that can be applied from adiabatic theorem

$$|\psi(x, t_1)|^2 \neq |\psi(x, t_0)|^2, \quad (50)$$

to quantum computation, from NP=QMA where

$$\text{QMA} \left(\frac{2}{3}, \frac{1}{3} \right) = \text{QMA} \left(\frac{1}{2} + \frac{1}{q(n)}, \frac{1}{2} - \frac{1}{q(n)} \right) = \text{QMA}(1 - 2^{-r(n)}, 2^{-r(n)}) \quad (51)$$

Bessonov, et. al. have demonstrated memristor state-alternating mechanics of bifurcation regimes and attractor, basin, and repeller waves where

$$\dot{x} = f(x, \lambda) \quad f: \mathbb{R}^n \times \mathbb{R} \rightarrow \mathbb{R}^n \text{ and } df_{x_0, \lambda_0} \quad (52)$$

for veryfine networks

$$x_{n+1} = f(x_n, \lambda) . \quad (53)$$

of Universal Computational Machines [UCM] proposed to be determined
 $a < b \in [0, 1]$,

such that

$$\frac{1}{b-a} = O(n^c), \quad (54)$$

therefore

$$\text{PSPACE} = \bigcup_{k \in \mathbb{N}} \text{SPACE}(n^k). \quad (55)$$

Wubs, Saito, et. al.[9] advance computation for qubit heat baths utilizing Landau-Zener

$$\text{DelE}=\text{E2(t)}-\text{E1(t)}-\text{at} \quad (56)$$

for

velocity of the heat bath phase

$$v_{LZ} = \frac{\frac{\partial}{\partial t}|E_2 - E_1|}{\frac{\partial}{\partial q}|E_2 - E_1|} \approx \frac{dq}{dt},$$

(57)

Therefore, time evolution is hypothesized per in the Von Neumann quantum groupings of Hopf algebras where

$$\begin{aligned} \text{Ad}_x \cdot y &= \sum_{(x)} x_{(1)} y S(x_{(2)}), \\ \Delta(x) &= \sum_{(x)} x_{(1)} \otimes x_{(2)} \end{aligned} \quad \text{and}$$

(58)

Monadically Parsons indicates the formula

$$S: N \rightarrow N - \{0\} \text{ for } (\forall M) \{ [0 \in M \ \& \ (\forall x) (x \in M \rightarrow Sx \in M)] \rightarrow N \subset M \}. [10]$$

(59)

Therefore the category commutations follow in u-arity that

$$T: C \rightarrow C \text{ for}$$

$$\eta: 1_C \rightarrow T. \quad (60)$$

9 Summary

In game theory and in information physics, structured wavefunctions in quantum games are demonstrated to have a topologically-ordered algebraic structure for universal algorithms in the evolutionary game computation. These are measured as quasiparticles [atoms] or probability fields of information categories, applicable to universal computers, and as categories of modular systems, for applied quantum mechanical regimes.

References

- [1] Kesten, 2006. "What is...Algorithm?", *Notices of the American Mathematical Society*, Providence, RI: American Mathematical Society, **53** (5): 572–573
- [2] Kendon, 2006. A random walk approach to quantum algorithms. arxiv.org extracted
- [3] Booth, 1974. *Modern Dogma & the Rhetoric of Assent* (The University of Chicago Press, 1974) Ward-Phillips Lectures in English Language and Literature, ISBN 9780226065724
- [4] Marblestone, A.H., Devoret, M. Exponential quantum enhancement for distributed addition with local nonlinearity. *Quantum Inf Process* **9**, 47–59 (2010). <https://doi.org/10.1007/s11128-009-0126-9>
- [5] Hochreiter, Schmidhuber, 1997. "Long Short-Term Memory", University website, extracted
- [6] Cheon, Tsutsui, 2005. Classical and Quantum Contents of Solvable Game Theory on Hilbert Space. arxiv.org, extracted
- [7] Freund, 2005. p-Adic Strings and their Applications. arxiv.org, extracted
- [8] Joulain, et. al., 2016. Quantum Thermal Transistor. *Physical Review Letters* **116** 200601
- [9] Wubs, Martijn; Saito, Keiji; Kohler, Sigmund; Hänggi, Peter; Kayanuma, Yosuke, 2006. Gauging a Quantum Heat Bath with Dissipative Landau-Zener Transitions. *Physical Review Letters*, vol. 97, Issue 20, id. 200404
- [10] Parsons, The Applicability of Mathematics, University website, extracted

ALGEBRAS GROUPS AND GEOMETRIES

INDEX VOL. 37, 2021

MAPPINGS PRESERVING SUM OF PRODUCTS $ab - ba^*$ ON FACTOR VON NEUMANN ALGEBRAS, 1

João Carlos da Motta Ferreira and Maria das Graças Bruno Marietto
Center for Mathematics, Computation and Cognition,
Federal University of ABC
Santa Adélia Street, 166,09210-170, Santo André, Brazil

SOME RESULTS ON WIENER INDEX, HYPER-WIENER INDEX AND ZAGREB INDEX, 15

B. Haghighi
Department of Chemistry, University of Neyshabur
Neyshabur, Razavi Khorasan Province, Iran
M.M. Nasrabadi
Department of Mathematics, University of Birjand
Birjand, Iran

STUDY OF A TYPE OF GENERALIZED BASIC HYPERGEOMETRIC SERIES, 27

Leda Galué
Centro de Investigación de Matemática Aplicada (CIMA)
Facultad de Ingeniería
Universidad del Zulia, Maracaibo, Venezuela

THE CAUSAL SPIRALS ON THE SPHERES OF LORENTZ-MINLOWSKI 3-SPACE R^3_1 , 81

M. Aydinalp
Manisa Celal Bayar University, Faculty of Arts and Sciences
Department of Mathematics, 45140, Manisa, Turkey
H.H. Ugurlu
Gazi University, Faculty of Education
Department of Secondary Education Science and Mathematics Teaching
Mathematics Teaching Program, 06560, Ankara, Turkey

ISONUMBERS AND RGB IMAGE ENCRYPTION, 103

Mamadou I. Wade and Tepper L. Gill

EECS Howard University
Washington, DC, 20059 U.S.A.

ON THE LAPLACIAN SPECTRUM OF THE COMAXIMAL GRAPHS, 120

Mojgan Afkhami

Department of Mathematics, University of Neyshabur
P.O. Box 91136-899, Neyshabur, Iran

Zahra Barati

Department of Mathematics, Kosar University of Bojnord
Bojnord, Iran

Kazem Khashyarmansh

Department of Pure Mathematics, Ferdowsi University of Mashhad
P.O. Box 1159-91775, Mashhad, Iran

**THE NUMBER OF PRODUCTS OF n ELEMENTS IN
A NONASSOCIATIVE ALGEBRA, 135**

Simon Davis

Research Foundation of Southern California
8861 Villa La Jolla Drive #13595
La Jolla, CA 92039

FRUTE LOOPS, 159

Tèmitópé Gbólàhàn Jaiyéolá

Adesola Adefemi Adeniregun

Department of Mathematics, Obafemi Awolowo University
Ile Ife 220005, Nigeria

Oyeyemi Oluwaseyi Oyebola

Faculty of Education, Brandon University
Brandon Manitoba, Canada

Adedayo Oke Adelakun

Department of Physics, Federal University of Technology
Akure, Ondo State, Nigeria

**ANALYTICAL SOLUTION OF AN INDUCED FIBER GRATING
RELATIVE HUMIDITY SENSOR, 181**

Mahboubeh Dehghani Sanij and Hosein Rooholamininejad

Shahid Bahonar University, Physics Faculty

Kerman, Iran 7616914111

Ali Reza Bahrampour

Sharif University of Technology, Department of Physics

Tehran, Iran 1458889694

HALIDON RINGS AND THEIR APPLICATIONS, 193

A. Telveenus

Kingston University of London International Study Centre

Stable Block, Kingston Hill Campus

KT2 7LB, UK

**ADVANCING COMPUTATIONAL SPACE VALUE THEORY [CSV
T] FOR MULTIVALENT GAME MECHANICS, 239**

Jonah Lissner

Canadian Journal of Pure and Applied Sciences

Computational Intelligence Group, University of Manitoba